June 30, 2006

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

Karen D. Cyr
General Counsel

FROM: Annette L. Vietti-Cook, Secretary /RA/

SUBJECT: STAFF REQUIREMENTS - SECY-06-0126 - PROPOSED RULEMAKING - POWER REACTOR SECURITY REQUIREMENTS (RIN 3150-AG63)

The Commission has approved publication of the proposed amendments to 10 CFR Parts 50, 72, and 73 in the *Federal Register*, subject to the comments and changes noted in the Commission votes, as modified by the comments below.

1. It is not necessary to seek public comment on the need to establish security requirements for the Emergency Response Data System.

2. PBL comment on page 320 (t)(4)(ii) and the bottom of page 926 should remain for the purpose of public comment in the proposed rule and the staff should clarify the basis for the cost benefit analysis.

3. PBL comment on page 460 should be deleted.

4. NJD vote, pp 99 - the staff should retain the rule text “to this part”.

5. NJD vote, pp 674 - the SOC text of the change description in Table 6 should be modified, rather than eliminated completely. The SOC text should be revised to indicate that this requirement would apply to both CAS and SAS operators (consistent with the Chairman’s and Comm. McGaffigan’s directed changes to the rule text).

6. EXM and GBJ votes - non-SGI versions of the guidance documents - to the extent practicable, the staff should make implementing guidance publically available, as appropriate, without causing undue delay in completion of this effort or other high priority security rulemakings.

7. The staff should take administrative action to withdraw all previously issued orders where appropriate.

8. JSM comments on pages 41 and 42 - retain original language.

9. EXM vote - (Add new Rule text to 73.55(b)(7) page) The language should read, “ (i)In

addition to ..... each licensee shall develop, ~~and~~ implement, and maintain an insider mitigation program.

The staff should plan to conduct more than one public meeting during the public comment period. Recent experience with other voluminous rule packages indicates that perhaps a second, or even a third, public meeting may be necessary to fully vet the issues addressed in this proposed rule.

In light of the status of NSIR and OGC staffs' ongoing interactions with the Department of Justice (DOJ) regarding the development of guidelines that will make new section 161A of the Atomic Energy Act effective, NSIR and OGC staffs should revise the proposed rule language for §§ 73.18 and 73.19 to reflect the current DOJ conceptual approach to section 161A, which would require licensees and certificate holders that are designated by the Commission to apply to the NRC for section 161A authority, if they wish to obtain the benefits of section 161A . The staff should make any other necessary conforming changes to the FRN's statement of considerations and to the supporting analyses to ensure consistency with the revised rule text. The staff should brief the Commission's technical assistants on the revised rule text prior to publication of the proposed rule.

Attachment: Commission Votes for SECY-06-0126

cc: Chairman Diaz
Commissioner McGaffigan
Commissioner Merrifield
Commissioner Jaczko
Commissioner Lyons
CFO
OCA
OPA
Office Directors, Regions, ACRS, ACNW, ASLBP (via E-Mail)
PDR

NOTATION VOTE

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: CHAIRMAN DIAZ

SUBJECT: **SECY-06-0126 - PROPOSED RULEMAKING - POWER REACTOR SECURITY REQUIREMENTS (RIN 3150-AG63)**

Approved w/comments xx Disapproved _____ Abstain _____

Not Participating _____

COMMENTS:

I approve publishing in the *Federal Register* the proposed amendments to 10 CFR Parts 50, 72, and 73 with appendices, and agree with staff's proposal to certify that the rule will satisfy the requirements of the Regulatory Flexibility Act, 5 U.S.C. 605 (b). Over the past several years the NRC has aggressively enhanced security at nuclear facilities through the issuance of security orders, security evaluations and lessons learned. This rulemaking is a culmination of those activities and will bring closure to these issues. In addition, the Energy Policy Act of 2005 has provided the agency with certain provisions to enhance the security programs at nuclear facilities. Edits are attached for incorporation into the rulemaking package. Further, the Order requirements addressed by the final rule should be rescinded.

SIGNATURE

June 20, 06

DATE

Entered on "STARS" Yes ✓ No ___

Table 2 - Part 73 Section 73.55

| | | |
|---|---|---|
| | (c)(1)(ii) Site-specific conditions that affect implementation of Commission requirements. | This requirement would be added to reflect the Commission's view that licensees must focus attention on site-specific conditions in the development and implementation of site plans, procedures, processes, response strategies, and ultimately, the licensee capability to achieve the performance objective of the proposed (b)(1). |
| | (c)(2) Protection of security plans. The licensee shall protect the approved security plans and other related safeguards information against unauthorized disclosure in accordance with the requirements of § 73.21. | This requirement would be added to emphasize the requirements for the protection of safeguards information in accordance with the requirements of § 73.21. |
| | (c)(3) Physical Security Plan. | This header would be added for formatting purposes. |

Table 2 - Part 73 Section 73.55

| | | |
|---|---|---|
| § 73.55(h)(1) Safeguards contingency plans must be in accordance with the criteria in Appendix C to this part, "Licensee Safeguards Contingency Plans." | (c)(5)(i) The licensee shall establish, maintain, and implement a Commission-approved safeguards contingency plan that describes how the criteria set forth in section II of Appendix C, "Licensee Safeguards Contingency Plans," to this part will be implemented. | This requirement would retain the current requirement of § 73.55(h)(1) to provide a safeguards contingency plan with minor revisions. Most significantly, the reference to Appendix C would be revised to reflect the reformatting of the proposed Appendix C which would have a section II that applies only to power reactors. |
| | (c)(5)(ii) The safeguards contingency plan must describe predetermined actions, plans, and strategies designed to intercept, challenge, delay, and neutralize threats up to and including the design basis threat of radiological sabotage. | This requirement would be added to generally describe the content of the Safeguards Contingency Plan. |
| | (c)(6) Implementing procedures. | This header would be added for formatting purposes. |

Table 2 - Part 73 Section 73.55

| | | |
|---|---|---|
| | (e)(4) Owner controlled area. The licensee shall establish and maintain physical barriers in the owner controlled area to deter, delay, or prevent unauthorized access, facilitate the early detection of unauthorized activities, and control approach routes to the facility. | This requirement would be added to provide a performance based requirement to provide enhanced protection outside the protected area relative to detecting, assessing, and delaying, a threat before reaching any area from which the threat could disable the personnel, equipment, or systems required to meet the performance objective and requirements described in the proposed paragraph (b). |
| | (e)(5) Isolation zone. | This header would be added for formatting purposes. |
| 10 CFR 73.55(c)(3) Isolation zones shall be maintained in outdoor areas adjacent to the physical barrier at the perimeter of the protected area... | (e)(5)(i) An isolation zone must be maintained in outdoor areas adjacent to the protected area perimeter barrier. The isolation zone shall be: | This requirement would retain the current requirement for an isolation zone. |

Table 2-Part 73 Section 73.55

| | | |
|---|---|---|
| | (g)(1)(vii) In response to specific threat information, implement a two-person (line-of-sight) rule for all personnel in vital areas so that no one individual is permitted unescorted access to vital areas. Under these conditions the licensee shall implement measures to verify that the two person rule has been met when a vital area is accessed. | This requirement would be added to require two specific actions to be taken by the licensee where credible threat information is provided. This proposed requirement, would first require that the two-person rule be implemented, and second, that measures be implemented to verify that the two-person rule is met when access to a vital area is gained. This proposed requirement would include those areas identified in the proposed (e)(8)(iv) to be protected as vital areas. |

Table 2 – Part 73 Section 73.55

| | | |
|---|---|---|
| § 73.55(h)(3) The total number of guards, and armed, trained personnel immediately available at the facility to fulfill these response requirements shall nominally be ten (10), unless specifically required otherwise on a case by case basis by the Commission; however, this number may not be reduced to less than five (5) guards. | (k)(3)(i)(A) The licensee shall determine the minimum number of armed responders necessary to protect against the design basis threat described in § 73.1(a), subject to Commission approval, and shall document this number in the approved security plans. | This requirement would be retained and revised to remove the specific minimum numbers of 10 but no less than 5, to provide a performance based requirement that meets the proposed requirement of (k)(1)(i). This proposed requirement would ensure that the licensee would provide the requisite number of armed responders needed to carry-out the protective strategy the effectiveness of which would be evaluated through annual exercises and triennial exercises observed by the Commission. |

Table 3 - Proposed Part 73 Section 73.56

| | | |
|---|---|---|
| | | licensees, applicants, and C/Vs to establish thresholds in interpreting the results of the psychological test, to aid in determining whether an individual would be required to be interviewed by a psychiatrist or licensed clinical psychologist under proposed paragraph (e)(4)(ii) of this section. |

Table 3 – Proposed Part 73 Section 73.56

| | | |
|---|---|---|
| | | history evaluation is completed.<br><br>The proposed rule would not would establish employment history requirements for individuals whose UAA has been interrupted for 30 or fewer days. Proposed § 73.56(h)(3) would require the entities who are subject to this section to obtain and review a personal history disclosure from the applicant for UAA that would address the period since the individual's last period of UAA was terminated. However, the licensee, applicant, or C/V would be permitted to forego conducting an employment history evaluation for individuals whose UAA has been |
| | | interrupted for such a short period, because there would be little to be learned. |

Table 5 – Proposed Part 73 Section 73.71

| | | |
|---|---|---|
| | appendix A to this part. Footnote: 2. Notifications to the NRC for the declaration of an emergency class shall be performed in accordance with § 50.72 of this chapter. | especially if this event is the opening action on an ineffectively coordinated multiple-target attack. Such notice may permit other licensees to escalate to a higher protective level in advance of an attack. The Commission would expect licensees to notify the NRC Operations Center as soon as possible after they notify local law enforcement agencies, but within 15 minutes. The Commission may consider the applicability of this requirement to other types of licensees in future rulemaking. |

Table 5 – Proposed Part 73 Section 73.71

| | | |
|---|---|---|
| | | Footnote 1 would provide a cross reference to Appendix A to Part 73 which contains NRC contact information.<br><br>Footnote 2 would remind licensees of their concurrent emergency declaration responsibilities under 10 CFR 50.72. |
| | (a)(1) When making a report under paragraph (a) of this section, the licensees shall: | The proposed rule would include this introductory statement, which provides a structure for the following list of information to be provided in the 15-minute report. |
| | (a)(1)(i) Identify the facility name; and | This requirement would be added to ensure the licensee's facility is clearly identified when a report is made. |

Table 5 – Proposed Part 73 Section 73.71

| | | |
|---|---|---|
| | appendix A to this part. Footnote: 2. Notifications to the NRC for the declaration of an emergency class shall be performed in accordance with § 50.72 of this chapter. | especially if this event is the opening action on an ineffectively coordinated multiple-target attack. Such notice may permit other licensees to escalate to a higher protective level in advance of an attack. The Commission would expect licensees to notify the NRC Operations Center as soon as possible after they notify local law enforcement agencies, but within 15 minutes. The Commission may consider the applicability of this requirement to other types of licensees in future rulemaking. |

Table 6 – Proposed Part 73, Appendix B

| | | |
|---|---|---|
| Appendix B, Paragraph I.B.2.b. Armed individuals, and central alarm station operators, in addition to meeting the requirement stated in Paragraph a. above, shall have no emotional instability that would interfere with the effective performance of assigned security job duties. The determination shall be made by a licensed psychologist or psychiatrist, or physician, or other person professionally trained to identify emotional instability. | B.3.b. A licensed clinical psychologist, psychiatrist, or physician trained in part to identify emotional instability shall determine whether armed members of the security organization in addition to meeting the requirement stated in Paragraph a. of this section, have no emotional instability that would interfere with the effective performance of assigned duties and responsibilities. | The requirement regarding emotional instability would be retained. ~~The phrase "Armed individuals, and central alarm station operators" would be replaced with the phrase "armed members of the security organization" for consistency with the terminology used in the proposed rule.~~ |

and alarm station operators

Table 8 - Part 73 Appendix G

| | | |
|---|---|---|
| | | or intelligence gathering efforts. Events reported under paragraphs I or II would require a followup written report. Events reported under paragraph III would not require a followup written report. |
| | I. Events to be reported as soon as possible, but no later than 15 minutes after discovery, followed by a written report within sixty (60) days.<br><br>(a) The initiation of a security response consistent with a licensee's physical security plan, safeguards contingency plan, or defensive strategy based on actual or imminent threat against a nuclear power plant. | Paragraph I would be added to establish the types events to be reported within 15 minutes. Because the identification of information relating to an actual or imminent potential threat could quickly result in an event, which may necessitate expedited Commission action (e.g., notification of other licensees or Federal authorities), a shorten reporting time would be required. This proposed requirement would also ensure that threat-related information would be made available to the Commission's threat assessment process |

Table 8 - Part 73 Appendix G

| | | |
|---|---|---|
| (2) Significant physical damage to a power reactor or any facility possessing SSNM or its equipment or carrier equipment transporting nuclear fuel or spent nuclear fuel, or to the nuclear fuel or spent nuclear fuel a facility or carrier possesses; or | II.(a)(2) Significant physical damage to any NRC-regulated power reactor or facility possessing strategic special nuclear material or to carrier equipment transporting nuclear fuel, or to the nuclear fuel or spent nuclear fuel facility which is possessed by a carrier; or | This requirement would be retained with minor editorial changes to improve clarity and readability and renumbered. The phrase "NRC-regulated" would be added to specify that all Commission licensed facilities and transport would be covered by this requirement. This change would simplify the language in this section while retaining the basic requirement. |

(including or spent nuclear fuel)

NOTATION VOTE

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: COMMISSIONER MCGAFFIGAN

SUBJECT: **SECY-06-0126 - PROPOSED RULEMAKING - POWER REACTOR SECURITY REQUIREMENTS (RIN 3150-AG63)**

Approved X w/comments & edits Disapproved _____ Abstain _____

Not Participating _____

COMMENTS:

See attached comments and edits.

Edward McGaffigan Jr.
SIGNATURE

June 28, 2006
DATE

Entered on "STARS" Yes X No ___

## Commissioner McGaffigan's Comments on SECY-06-0126

I approve publication of this proposed rulemaking for public comment, and agree with the staff's proposal to certify that this rule satisfies the requirements of the Regulatory Flexibility Act, 5 U.S.C. 605(b). I would like to laud the work of the staff in putting together a well reasoned, organized and thoroughly conceived rule. In particular, the staff has made a constructive proposal for facilities that will use MOX fuel, and that is consistent with the Commission's action in a recent adjudication. I look forward to comments on the requirements contained in the proposed rule.

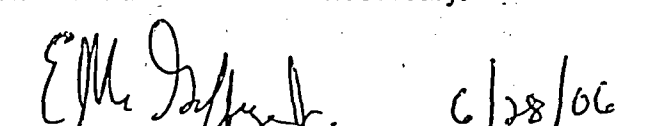
Having said that, I believe the rule should explicitly address the need for mitigation of potential insider threats. While the proposed rule text incorporates many of the elements that would serve to identify potential insider threats, additional language is needed to explicitly require the development and implementation of an Insider Mitigation Program and tie together the necessary program elements to allow for meaningful comment. As such, I am attaching proposed additional rule text language to be included in 10 CFR 73.55(b)(7).

The staff's modification to the Appendix B requirements regarding evaluations designed to identify emotional instability in critical personnel, is too narrowly drawn and should be expanded to at least include alarm station operators. Just like armed members of the security organization, CAS and SAS operators serve a critical function, the impairment of which could constitute a significant risk.

Modifications to Appendix G requirements for "Reportable Safeguards Events" should be more narrowly drafted to properly limit the scope of information that falls within the 4-hour reporting requirement set forth in Section III. As currently written, the use of "or other information" in subsection (a) of Section III is too open-ended.

The staff, with assistance from Idaho National Laboratory, has an ambitious plan to revise and update relevant guidance documents. I agree with Commissioner Jaczko that the staff should strive to make as much of the implementing guidance as possible publicly available. I recognize that some elements of the guidance will be considered Safeguards Information or sensitive unclassified information, and therefore could not be included in a public document. In such cases, the public version of the document could indicate that additional guidance is provided in the Safeguards Information version of the document. The staff should provide the guidance documents to the Commission for information when they are issued for comment.

Finally, while this rule will go a long way towards creating the necessary stability for applicants and licensees, particularly as we prepare for new reactor licensing, the security orders addressed in large part through this rulemaking should remain in place. Rescission of these orders automatically upon completion of the final rule is neither necessary nor prudent. When this rule is final, existing licensees will be required to examine their security plans to ensure compliance with the new regulations. While most licensees may not need to make any modifications, there is a chance that some changes will be necessary or they will need to seek relief. Following this review, some licensees may, in accordance with the terms of the orders, seek relaxation of order provisions or amendment of their licenses if necessary.



Edward McGaffigan, Jr. (Date) 6/28/06

**ADD new Rule text to 73.55(b)(7):**

**(i)** In addition to the access authorization program required above, and the fitness-for-duty program required in part 26 of this chapter, each licensee shall develop and implement an insider mitigation program.

**(ii)** The insider mitigation program must be designed to oversee and monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorization to a protected or vital area and implement defense-in-depth methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, the licensee capability to prevent significant core damage or spent fuel sabotage.

**ADD new Rule text and Considerations to Table 2:**

| Current Requirement | Proposed Requirement | Considerations |
|---|---|---|
| | **73.55(b)(7)(i)** In addition to the access authorization program required above, and the fitness-for-duty program required in part 26 of this chapter, each licensee shall develop and implement an insider mitigation program. | This proposed requirement would be added to establish the insider mitigation program (IMP). The licensee's IMP should integrate specific elements of the licensee AA and FFD programs to focus those elements on identifying potential insider threats and denying the opportunity for an insider to gain or retain access at an NRC licensed facility. |

| | | |
|---|---|---|
| | **73.55(b)(7)(ii)** The insider mitigation program must be designed to oversee and monitor the initial and continuing trustworthiness and reliability of any individual granted or retaining unescorted access authorization to a protected or vital area and implement defense-in-depth methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, the licensee capability to prevent significant core damage or spent fuel sabotage. | This proposed requirement would be added to provide a performance based requirement for the design and content of the IMP. The Commission has concluded that, by itself, the initial determination of trustworthiness and reliability is not adequate to minimize the potential opportunity for an insider to gain or retain access, and that only through continual re-evaluation of the information obtained through these processes can the licensee provide the level of assurance necessary. The Commission has also determined that defense-in-depth would be provided through the integration of physical protection measures with access authorization and fitness-for-duty program elements, to ensure the licensee capability to identify and mitigate the potential activities of an insider, such as, but not limited to, tampering. The Commission does not intend that a licensee would limit the IMP to any one or more elements, but rather that the licensee would identify and add additional elements as necessary to ensure the site's IMP satisfies the performance requirements specified by the Commission. |

| | | |
|---|---|---|
| | | The Commission has determined that no one element of the physical protection program, access authorization program, or fitness-for-duty program would, by itself, provide the level of protection against the insider necessary to meet the performance objective of the proposed paragraph (b) and therefore, the effective integration of these three programs is a necessary requirement to achieve defense-in-depth against the potential insider. |

NRC Form 754) to the list of sections and forms with Office of Management of Management Budget (OMB) information collection requirements. A corrective revision to § 73.8 would also be made to reflect OMB approval of existing information collection requirements for NRC Form 366 under existing § 73.71.

- Section 73.70, "Records" would be revised to reference the appropriate revised paragraph numbers in proposed § 73.55 regarding the need to retain a record of the registry of visitors.

Additionally, § 73.81(b), "Criminal penalties" which sets forth the sections within Part 73 that are not subject to criminal sanctions under the AEA, would remain unchanged since willful violations of the newly proposed §§ 73.18, 73.19, and 73.58 may be subject to criminal sanctions.

Appendix B and Appendix C to Part 73 require special treatment in this rulemaking to preserve, with a minimum of conforming changes, the current requirements for licensees and applicants to whom this proposed rule would not apply. Accordingly, section I through V of Appendix B would remain unchanged, and the proposed new language for power reactors would be added as section VI. Appendix C would be divided into two sections, with Section I maintaining all current requirements, and Section II containing all proposed requirements related to power reactors.

## II. Rulemaking Initiation

On July 19, 2004, NRC staff issued a memorandum entitled "Status of Security-Related Rulemaking" (accession number ML041180532) to inform the Commission of plans to close former security-related actions and replace them with a comprehensive rulemaking plan to modify physical protection requirements for power reactors. This memorandum described rulemaking efforts that were suspended by the terrorist activities of September 11, 2001, and

summarized the security-related actions taken following the attack. In response to this memorandum, the Commission directed the staff in an August 23, 2004, Staff Requirements Memorandum (SRM) (COMSECY-04-0047, accession number ML042360548) to forego the development of a rulemaking plan, and provide a schedule for the completion of security-related rulemakings. The staff provided this schedule to the Commission by memorandum dated November 16, 2004 (accession number ML043060572). Subsequently, the staff revised its plans to amend the Part 73 security requirements to include a requirement for licensees to assess and manage site activities that could compromise either safety or security (i.e., the safety/security interface requirements). This revision is discussed in a memorandum dated July 29, 2005 (accession number ML051800350). Finally, by memorandum dated September 29, 2005 (COMSECY-05-0046, accession number ML052710167), the staff discussed its plans to incorporate select provisions of the EPAct 2005 into the power reactor security requirements rulemaking. In COMSECY-05-0046, dated November 1, 2005 (accession number ML053050439), the Commission approved the staff's approach in incorporating the select provisions of EPAct 2005.

## III. Proposed Regulations

note: Sec 653 of EPAct added new Sec 161A. to AEA of 1954 as amended (AEA)

This section describes significant provisions of this rulemaking:

1. EPAct 2005 weapons requirements. The new §§ 73.18 and 73.19 would contain requirements to implement provisions of Sec. 161A. of the AEA. In § 73.18, the NRC would propose firearms background check requirements and would also propose a new NRC Form 754 for licensee security personnel's submission to accomplish these firearms background checks under the FBI's NICS database. In § 73.19, the NRC would propose requirements to support a licensee obtaining enhanced weapons under an ATF firearms license.

concerning the transfer, receipt, possession, transport, and use of enhanced weapons and the requirements for firearms background checks for security personnel.

2. Safety/Security interface requirements. These requirements are located in proposed § 73.58. The safety/security requirements are intended to explicitly require licensee coordination of potential adverse interactions between security activities and other plant activities that could compromise either plant security or plant safety. The proposed requirements would direct licensees to assess and manage these interactions so that neither safety nor security is compromised. These proposed requirements address, in part, a Petition for Rulemaking (PRM 50-80) that requested the establishment of regulations governing proposed changes to the facilities which could adversely affect the protection against radiological sabotage.

3. EPAct 2005 additional requirements. The EPAct 2005 requirements that would be implemented by this proposed rulemaking, in addition to the weapons-related additions described above, consist of new requirements to perform force-on-force exercises, and to mitigate potential conflicts of interest that could influence the results of NRC-observed force-on-force exercises. These proposed new requirements would be included in proposed § 73.55 and Appendix C to Part 73.

4. Accelerated notification and revised four-hour reporting requirements. This proposed rule contains accelerated security notification requirements (i.e., within 15 minutes) in proposed § 73.71 and Appendix G to Part 73 for attacks and imminent threats to power reactors. The proposed accelerated notification requirements are similar to what was provided to the industry in NRC Bulletin 2005-02, "Emergency Preparedness and Response Actions for Security-Based Events," dated July 18, 2005. The proposed rule also contains two new four-

hour reporting requirements. The proposed rule would direct licensees to report to the NRC information pertaining to suspicious activities as described in the proposed requirement. The proposed rule would also include a new four-hour reporting requirement for tampering events that do not meet the current threshold for one-hour reporting.

5. Mixed-oxide (MOX) fuel requirements. These requirements would be incorporated into proposed § 73.55 for licensees who propose to use MOX fuel in their reactor(s). These proposed requirements are in lieu of unnecessarily rigorous Part 73 requirements (e.g., §§ 73.45 and 73.46), which would otherwise apply because of the mixed oxide (MOX) fuel's low plutonium content and the weight and size of the MOX fuel assemblies. The proposed MOX fuel security requirements are intended to be consistent with the approach implemented by at Catawba through the MOX lead test assembly effort.
A
Nuclear Station

6. Cyber-security requirements. This proposed rule would contain more detailed programmatic requirements for addressing cyber security at power reactors, which build on the requirements imposed by the February 2002 order. The proposed cyber-security requirements are designed to be consistent with ongoing industry cyber-security efforts.

7. Mitigating strategies. The proposed rule would require licensees to develop specific guidance and strategies to maintain or restore core cooling, containment, and spent fuel pool cooling capabilities using existing or readily available resources (equipment and personnel) that can be effectively

rule would also add new requirements, including predefined provisions for the suspension of safeguards measures for severe weather conditions that could result in life-threatening situations for security personnel (e.g., tornadoes, floods, and hurricanes), and reduced overly-prescriptive requirements through the inclusion of performance-based language to allow flexibility in the methods used to accomplish requirements.

## IV. Section-by-Section Analysis

### IV.1. New weapons requirements.

This proposed rulemaking would implement new weapons requirements that stem from the EPAct 2005. This is the only portion of this proposed rulemaking that involves facilities other than nuclear power reactors. The newly proposed weapons requirements would apply to power reactors and facilities authorized to possess a formula quantity or greater of strategic special nuclear material whose security plans are governed by §§ 73.20, 73.45, and 73.46. The new requirements would be in three different sections and an NRC Form:

- Revised proposed § 73.2 "Definitions" would include the utilization of
- Proposed § 73.18, "Firearms background checks for armed security personnel"
- Proposed § 73.19, "Authorization for use of enhanced weapons"
- Proposed NRC Form 754, "Armed Security Personnel Background Check"

Proposed § 73.18 would contain requirements that implement provisions of new Sec. 161A. of the AEA (under Sec. 653 of the EPAct 2005) concerning firearms background checks for armed security personnel. This new section would require background checks that include fingerprinting and checks against the FBI's NICS. Security personnel protecting power reactors and Category I SSNM facilities are currently subject to background checks, including fingerprints, because they have unescorted access at such facilities. However, these security

personnel have not previously been subject to a check against the NICS database because the access authorization background checks were not intended to perform the entire scope of checks required for firearms possession. Although licensee security personnel possessing weapons have always had to comply with the federal regulations for firearms possession, the NRC did not have the authority to perform these checks. This proposed requirement would provide a process for conducting the NICS checks.

Implementation of the proposed § 73.18 background checks would be via proposed NRC Form 754, which armed security personnel would be required to complete. The NRC would forward the NRC Form 754 information to the FBI for evaluation, and upon completion of the FBI evaluation, inform licensees of the result. The result would be either "proceed," "denied," or "delayed." Proposed § 73.18 would be structured to readily enable revisions in the future, should NRC decide to expand the proposed rulemaking provisions to apply to other types of facilities and licensees.

Proposed § 73.19 would contain requirements that implement provisions of new Sec. 161A. of the AEA concerning the use of enhanced weapons to protect facilities, radioactive material, or other property as determined by the Commission. The proposed § 73.19 would authorize (not require) power reactors and facilities authorized to possess formula quantities of strategic special nuclear material (i.e., Category I SSNM) to incorporate the use of enhanced weapons into their protective strategy. Affected Category I licensees would include production facilities, spent fuel reprocessing or recycling facilities, fuel fabrication facilities, and uranium enrichment facilities. However, this would not include hot cell facilities, independent spent fuel storage installations, monitored retrievable storage installations, and a geologic repository operations area. The NRC plans to address whether the deployment of enhanced weapons is appropriate for these and other types of facilities, radioactive material, or other property in separate rulemaking(s).

Furthermore, Sec. 161A. of the AEA takes effect upon the issuance of guidelines by the Commission, with the approval of the Attorney General. As indicated previously, the Commission intends to provide public notice of the issuance of these guidelines in a separate *Federal Register* notice to be published no later than the final rule on this action.

To implement the new weapons provisions, three new terms would be added to § 73.2: *covered weapon*, *enhanced weapon*, and *standard weapon.*

Indent > The proposed new weapons requirements and supporting discussion for the proposed language are set forth in more detail (including the proposed new definitions) in Table 1.

IV.2. Section 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage."

Proposed § 73.55 contains security program requirements for power reactor licensees. The security program requirements in § 73.55 would apply to all nuclear power plant licensees that hold a 10 CFR Part 50 license and to applicants who are applying for either a Part 50 license or a Part 52 combined license. Paragraph (a) of § 73.55 would identify the licensees and applicants for which the requirements apply, and the need for submitting to NRC (for review and approval) a "Physical Security Plan," a "Training and Qualification Plan," and a "Safeguards Contingency Plan." Paragraph (b) of § 73.55 would set forth the performance objectives that govern power reactor security programs. The remaining paragraphs of § 73.55 would implement the detailed requirements for each of the security plans, as well as for the various features of physical security.

This section would be extensively revised in an effort to make generically applicable security requirements imposed by Commission orders issued after the terrorist attacks of September 11, 2001, based upon experience and insights gained by the Commission during implementation, fulfill certain provisions of the ~~Energy Policy Act of~~ 2005, and add several new



Elan

requirements that resulted from evaluation insights from implementation of the security orders, review of site security plans, and implementation of the enhanced baseline inspection program and force-on-force exercises. The proposed regulations would require an integrated security plan that begins at the owner controlled area boundary and would implement defense-in-depth concepts and protective strategies based on protecting target sets from the various attributes of the design basis threat. Notable additions to the proposed § 73.55 are summarized below:

Cyber Security Requirements

The current security regulations do not contain requirements related to cyber security. Subsequent to the events of September 11, 2001, the NRC issued orders to require power reactor licensees to implement measures to enhance cyber security. These security measures required an assessment of cyber systems and the implementation of corrective measures sufficient to provide protection against the cyber threats at the time the orders were issued.

The proposed requirements maintain the intent of the security order by establishing the requirement for a cyber security program to protect any system that, if compromised, can adversely impact safety, security or emergency preparedness.

Requirements for CAS and SAS to Have Functionally Equivalent Capabilities Such That No Single Act Can Disable the Function of CAS and SAS

Current regulatory requirements ensure that both CAS and SAS have equivalent alarm annunciation and communication capabilities, but do not explicitly require equivalent assessment, monitoring, observation, and surveillance capabilities. Further, the current requirement of § 73.55(e)(1) states "All alarms required pursuant to this part must annunciate in a continuously manned central alarm station located within the protected area and in at least one other continuously manned station not necessarily onsite, so that a single act cannot remove the capability of calling for assistance or otherwise responding to an alarm." The Commission orders added enhanced detection and assessment capabilities, but did not require

equivalent capabilities for both CAS and SAS. The security plans approved by the Commission on October 29, 2004, varied, due to the performance-based nature of the requirements, with respect to how the individual licensees implemented these requirements, but all sites were required to provide a CAS and SAS with functionally equivalent capabilities to support the implementation of the site protective strategy.

The proposed rule extends the requirement for no single act to remove capabilities to the key functions required of the alarm stations and would require licensees to implement protective measures such that a single act would not disable the intrusion detection, assessment, and communications capabilities of both the CAS and SAS. This proposed requirement would ensure continuity of response operations during a security event by ensuring that the detection, assessment, and communications functions required to effectively implement the licensee's protective strategy are maintained despite the loss of one or the other alarm station. For the purposes of assessing the regulatory burden of this proposed rule, the NRC assumed that all licensees would require assessments and approximately one third of the licensees would choose to implement hardware modifications.

The NRC has concluded that protecting the alarm stations such that a single act does not disable the key functions would provide an enhanced level of assurance that a licensee can maintain detection, assessment and communications capabilities required to protect the facility against the design basis threat of radiological sabotage. For new reactor licensees, licensed after the publication of this rule, the Commission would require CAS and SAS to be designed, constructed, and equipped with equivalent standards.

Uninterruptible Power for Intrusion Detection and Assessment Systems

Current regulatory requirements require back-up power for alarm annunciation and non-portable communication equipment, but do not require this back-up power to be uninterruptible. Although not specifically required, many licensees have installed uninterruptible power to their

security systems for added reliability of these electronic systems. However, the Commission has not required uninterruptible power for assessment systems. For the purposes of assessing the regulatory burden of this proposed rule, the NRC assumed that only a small number of licensees would require hardware modifications to meet this proposed requirement.

Through implementation of the Commission-approved security plans, baseline inspections, and force-on-force testing, the NRC has concluded that uninterruptible back-up power would provide an enhanced level of assurance that a licensee can maintain detection, assessment and communication capabilities required to protect the facility against the design basis threat of radiological sabotage. This new requirement would reduce the risk of losing detection, assessment, and communication capabilities during a loss of the normal power supply.

"Video-Capture" Capability

Current regulatory requirements address the use of closed circuit television systems, but do not explicitly require them. Although not specifically required, all licensees have adopted the use of video surveillance in their site security plans. Many of the licensees have adopted advanced video surveillance technology to provide real-time and play-back/recorded video images to assist security personnel in determining the cause of an alarm annunciation. For the purposes of assessing the regulatory burden of this proposed rule, the NRC assumed that a small percentage of licensees would require hardware modifications to comply with this proposed requirement for advanced video surveillance technology.

Through implementation of the Commission-approved security plans, baseline inspections, and force-on-force testing, the NRC has concluded that advanced video technology would provide an enhanced level of assurance that a licensee can assess the cause of an alarm annunciation and initiate a timely response capable of defending the facility against

2001. Licensees have always been required to ensure that any changes to safety functions, systems, programs, and activities do not have unintended consequences on other facility safety functions, systems, programs, and activities. Likewise, licensees have been required to ensure that any changes to security functions, systems, programs, and activities do not have unintended consequences on other facility security functions, systems, programs, and activities. However, the Commission has concluded that the pace, number, and complexity of these security changes warrants the establishment of a more formal program to ensure licensees properly assess the safety/security interface in implementing these changes.

On April 28, 2003, the Union of Concerned Scientists and the San Luis Obispo Mothers for Peace submitted a petition for rulemaking (PRM-50-80) requesting that, in part, the NRC's regulations establishing conditions of licenses and requirements for evaluating proposed changes, tests, and experiments for nuclear power plants be amended to require licensee evaluation of whether the proposed changes, tests, and experiments cause protection against radiological sabotage to be decreased and, if so, that the changes, tests, and experiments only be conducted with prior NRC approval. In SECY-05-0048, dated March 28, 2005, the NRC staff recommended that the Commission approve rulemaking for the requested action, but did not necessarily endorse the specific amendments suggested by the petition. In SECY-05-0048, dated June 28, 2005, the Commission directed the staff to develop the technical basis for such a rule and to incorporate its provisions within the ongoing power reactor security requirements rulemaking. This proposed rule addresses, in part, the petitioner's request by incorporating proposed § 73.58 within this rulemaking.

The Commission has determined that the proposed safety/security interface rule requirements are necessary because the current regulations do not specifically require evaluation of the effects of plant changes on security or the effects of security changes on plant safety. Further, current regulations do not require communication about the implementation

and timing of changes, which would promote awareness of the effects of changing facility conditions and result in appropriate assessment and response.

The NRC is aware of a number of occurrences of adverse safety/security interactions at nuclear power plants over the years to justify consideration of a new rule. Examples of adverse interactions include: (1) Inadvertent security barrier breaches while performing maintenance activities (e.g., cutting of pipes that provided uncontrolled access to vital areas, removing ventilation fans or other equipment from vital area boundary walls without taking compensatory measures to prevent uncontrolled access into vital areas); (2) Blockage of bullet resisting enclosure's (or other defensive firing position's) fields of fire; (3) Erection of scaffolding and other equipment without due consideration of its impact on the site's applicable physical protection strategy; and (4) Staging of temporary equipment within security isolation zones.

Security could also adversely affect operations because of inadequate staffing of security force personnel on backshifts, weekends, and holidays, to support operations during emergencies (e.g., opening and securing vital area access doors to allow operations personnel timely access to safety-related equipment). Also, security structures, such as vehicle barriers, delay barriers, rerouted isolation zones, or defensive shields could adversely affect plant equipment such as valve pits, fire stations, other prepositioned emergency equipment, blowout panels, or otherwise interfere with operators responding to plant events.

The NRC considered many factors in developing this proposed new requirement. One of the factors considered is that existing change processes are focused on specific areas of plant activities, and that implementation of these processes is generally well understood by licensees. An example is found in § 50.54(p), which provides that a reactor licensee may make changes to its safeguards contingency plans without Commission approval provided that the changes do not decrease the safeguards effectiveness of the plan. Similarly, § 50.65(a)(4) provides that a reactor licensee shall assess and manage the increase in risk that may result

from proposed maintenance activities. However, neither §§ 50.54(p) (security) nor 50.65(a)(4) (safety) require that an assessment for potential adverse impacts on safety/security interface be made before the proposed changes are implemented. The proposed § 73.58 would address this gap by requiring that, before implementing allowed changes, licensees must assess the changes with respect to the safety/security interface and, if potential adverse interactions are identified, take appropriate compensatory and/or mitigative action before making the changes.

The proposed rule reflects a performance-based approach and language which is sufficiently broad that, in addition to operating power reactors, it could be applied to other classes of licensees in separate rulemaking(s), if conditions warrant. In addition to the requirements in proposed § 73.58, a new definition for safety/security interface would be added to § 73.2.

Table 4 sets forth the proposed § 73.58 language and provides the supporting discussion for the proposed language, including a new definition for *safety/security interface* that would be added to § 73.2.

IV.5. Section 73.71 "Reporting of safeguards events."

The events of September 11, 2001, emphasized the need for the capability to respond to coordinated attacks that could pose an imminent threat to national infrastructure such as nuclear power reactor sites. Prompt licensee notification to the NRC of a security event involving an actual or imminent threat would initiate the NRC's alerting mechanism for other nuclear facilities in recognition that an attack or threat against a single facility may be the prelude to attacks or threats against multiple facilities. In either case, timely communication of this event to the NRC, and the NRC's communication of the threat or attack to other licensees could reduce the adversaries ability to engage in coordinated attacks and would strengthen the licensees' response posture. NRC would also initiate notifications to the Homeland

Security/Federal response networks for an "Incident of National Significance," as defined by the National Response Plan (NRP).

Currently, § 73.71(b)(1) requires power reactor licensees to notify the NRC within one hour of discovery, as described in Paragraph I of Appendix G to 10 CFR Part 73, "Reportable safeguards events." In addition, § 50.72 establishes reporting requirements for events requiring an emergency declaration in accordance with a licensee's emergency plan. Licensee notification under § 50.72(a)(3) is required only after the threat is assessed, an "Emergency Class" is declared, and initial notification of appropriate State and local agencies are completed first (i.e., not upon discovery). The current timing of requirements of this notification would not allow the NRC to warn other licensees of a potential threat to their facilities in a prompt manner to allow other licensees to change their security posture in advance of a threat or potential attack. The Commission has previously advised licensees of the need to expedite their initial notification to the NRC. The proposed accelerated notification requirements are similar to those provided to licensees in NRC Bulletin 2005-02, "Emergency Preparedness and Response Actions for Security-Based Events," dated July 18, 2005.

The proposed amendments to § 73.71 would add a new expedited notification requirement for licensees subject to the provisions of § 73.55 to notify the NRC Operations Center as soon as possible after the discovery of an imminent or actual threat against the facility as described in Appendix G, but not later than 15 minutes after discovery. The proposed amendments to § 73.71 and Appendix G would also add two additional four-hour notification requirements for suspicious events and tampering events not otherwise covered under Appendix G. The proposed § 73.71 would retain the requirement for the licensee to maintain a continuous communications channel for one-hour notifications upon request of the NRC. The proposed rule would not require a continuous communications channel for four-hour notifications, because of the lesser degree of urgency of these events. For 15-minute

Table 11 (See Section VIII) is a cross-reference showing where individual requirements of the current regulation would be in the proposed regulation.

IV.8. Appendix G to Part 73, "Reportable Safeguards Events."

Proposed Appendix G to Part 73 provides requirements regarding the reporting of safeguards events. Proposed Appendix G would contain changes to support the revised and accelerated reporting requirements which would be incorporated into this rulemaking. Proposed Appendix G would also contain revised four-hour reporting requirements that would require licensees to report to the NRC information of suspicious surveillance activities, attempts at access, or other information. Following September 11, 2001, the NRC issued guidance requesting that licensees report suspicious activities near their facilities to allow assessment by the NRC and other appropriate agencies. The proposed new reporting requirement will clarify this expectation to assure consistent reporting of this important information. Additionally, the proposed rule contains an additional four-hour reporting requirement for tampering events that do not meet the threshold for reporting under the current one-hour requirements. The proposed reporting requirements for tampering events will allow NRC assessment of these events. Table 8 sets forth the proposed amendments to Appendix G and provides the supporting discussion for the proposed language.

IV.9 Conforming and Corrective Changes.

The following conforming changes would also be made: §§ 50.34 and 50.54 (references to the correct paragraphs of revised Appendix C of Part 73), § 50.72 (changes to § 73.71 reports), §§ 72.212 and 73.70 (references to the correct paragraphs due to renumbering of § 73.55), and § 73.8 (adding § 73.18, § 73.19, and revised to reflect new NRC form 754 to

reflect recordkeeping or reporting burden). A corrective change would also be made to § 73.8 to reflect an existing recordkeeping or reporting burden for NRC Form 366 under § 73.71. However, no changes would be made to § 73.81(b) (due to the new §§ 73.18, 73.19, and 73.58), because willful violations of §§ 73.18, 73.19, and 73.58 may be subject to criminal penalties.

Table 1 - Proposed Sections 73.18 and 73.19

Firearms background check for armed security personnel and authorization for use of enhanced weapons.

| PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|
| § 73.18 Firearms background check for armed security personnel. | This new section would implement the firearms background check requirements of the new § 161A.b. of the Atomic Energy Act of 1954, as amended |
| (a) *Introduction.* (1) Licensees and certificate holders listed under paragraph (b) of this section shall ensure that a firearms background check is completed in accordance with this section for all security personnel assigned duties requiring access to a covered weapon at the licensee's or certificate holder's facility. | This section would require a firearms background check for all security personnel with access to covered weapons (i.e., armed duties) [see also new definition of *covered weapon* in § 73.2 at the end of this Table]. These background checks would only be required for security personnel who are protecting certain Commission-regulated facilities [specified in paragraph (b)].<br>The Commission considers duties "requiring access to any covered weapon" would include such duties as: security operations and training and weapons' maintenance, handling, accountability, transport, and use. |

| | |
|---|---|
| § 73.18(a)(2) Licensees and certificate holders are not required to reperform a firearms background check for security personnel who have been employed by the licensee or certificate holder (or a contractor thereto) and previously completed a firearms background check under the provisions of Sec. 161A. of the Atomic Energy Act of 1954, as amended, after [insert date of publication of the Sec. 161A. guidelines in the *Federal Register*]. | Licensees and certificate holders would not be required to repeat firearms background checks for personnel assigned armed duties at their facility as of the effective date of a final rule. This discretion would apply to security personnel employed at the licensee's or certificate holder's facility and who have previously completed a firearms background check as required by an order issued under the authority of § 161A. of the AEA. The security personnel may be employed directly by the licensee or certificate holder or by a contractor to the licensee or certificate holder. |

| | |
|---|---|
| § 73.18(b) *Applicability.* This section applies to the following classes of Commission licensees or certificate holders –<br>(1) Power reactor facilities; and<br>(2) Facilities authorized to possess a formula quantity or greater of strategic special nuclear material with security plans subject to §§ 73.20, 73.45, and 73.46. | This paragraph would limit the firearms background checks to security personnel protecting two classes of Commission-regulated facilities. Therefore, this section would apply to all current power reactors and to two current fuel cycle facilities authorized to possess Category I SSNM. This section would also apply to future power reactor facilities and future Category I SSNM facilities, including: production facilities, spent fuel reprocessing or recycling facilities, fuel fabrication facilities (high-enriched uranium or MOX fuel), and uranium enrichment facilities.<br>The Commission may consider applying this section to other types of reactor, byproduct material, or special nuclear material facilities (e.g., Category II or III SNM, hot cell, independent spent fuel storage, or geologic repository operations area facilities) in separate rulemakings. |

| | |
|---|---|
| § 73.18(c) *Firearms background check.* (1) Licensees and certificate holders described in paragraph (b) of this section shall ensure that each person who receives, possesses, transports, or uses a covered weapon in their official duties completes a firearms background check. The firearms background check must verify whether security personnel are prohibited from shipping, transporting, possessing, or receiving a covered weapon under applicable Federal or State law. The background check must include –<br>(i) The submission of fingerprints; and<br>(ii) A check under the Federal Bureau of Investigation's (FBI's) National Instant Criminal Background Check System (NICS) database established pursuant to Sec. 103.(b) of the Brady Handgun Violence Prevention Act. | This paragraph would require licensees and certificate holders to ensure that security personnel with "armed duties" shall first complete a firearms background check. This check would verify that such security personnel are not prohibited from possessing or receiving firearms under applicable laws. The requirement to perform background checks of armed security personnel at NRC-regulated entities against the Brady Bill (i.e., NICS) database arises from § 161A. of the AEA. The background check would consist of two parts as required by § 161A. of the AEA. |

Handgun Violence prevention Act

| | | |
|---|---|---|
| | (c)(1)(i) How the physical protection program will prevent significant core damage and spent fuel sabotage through the establishment and maintenance of a security organization, the use of security equipment and technology, the training and qualification of security personnel, and the implementation of predetermined response plans and strategies; and | This requirement would be added to describe the performance based requirement to be met by the physical protection program and the basic elements of the system that must be described in the security plans. |

| | | |
|---|---|---|
| | (c)(1)(ii) Site-specific conditions that affect implementation of Commission requirements. | This requirement would be added to reflect the Commission's view that licensees must focus attention on site-specific conditions in the development and implementation of site plans, procedures, processes, response strategies, and ultimately, the licensee capability to achieve the performance objective of the proposed (b)(1). |
| | (c)(2) Protection of security plans. The licensee shall protect the approved security plans and other related safeguards information against unauthorized disclosure in accordance with the requirements of § 73.21. | This requirement would be added to emphasize the requirements for the protection of safeguards information in accordance with the requirements of § 73.21. |
| | (c)(3) Physical Security Plan. | This header would be added for formatting purposes. |

| | | |
|---|---|---|
| | | be authorized are governed by State laws and nothing in this proposed rule should be interpreted to mean or require anything that would contradict such state law. The term "it" is replaced with the phrase "deadly force" to more clearly described the action described. |
| | (k)(3) The licensee shall provide an armed response team consisting of both armed responders and armed security officers to carry out response duties, within predetermined time lines. | This requirement would be added to provide a performance based requirement that would retain the current requirement for armed responders and add a category of armed security officer to clarify the division of types of armed response personnel and their roles. |
| | (k)(3)(i) Armed Responders. | This header would be added for formatting purposes. |

| | | |
|---|---|---|
| § 73.55(h)(3) The total number of guards, and armed, trained personnel immediately available at the facility to fulfill these response requirements shall nominally be ten (10), unless specifically required otherwise on a case by case basis by the Commission; however, this number may not be reduced to less than five (5) guards. | (k)(3)(i)(A) The licensee shall determine the minimum number of armed responders necessary to protect against the design basis threat described in § 73.1(a), subject to Commission approval, and shall document this number in the approved security plans. | This requirement would be retained and revised to remove the specific minimum numbers of 10 but no less than 5, to provide a performance based requirement that meets the proposed requirement of (k)(1)(i). This proposed requirement would ensure that the licensee would provide the requisite number of armed responders needed to carry-out the protective strategy the effectiveness of which would be evaluated through annual exercises and triennial exercises observed by the Commission. |

| | | |
|---|---|---|
| | | standardized, objective test to facilitate the psychological re-assessments that would be required under proposed § 73.56(i)(1)(v). Comparing scores on a standardized, objective test to identify indications of any adverse changes in the individual's psychological status is simplified when the testing that is performed for a re-assessment is similar to or the same as previous testing that was conducted under this section, particularly when the clinician who conducts the re-assessment did not conduct the previous testing.<br><br>The proposed paragraph would also require |

| | | |
|---|---|---|
| | | licensees, applicants, and C/Vs to establish thresholds in interpreting the results of the psychological test, to aid in determining whether an individual would be required to be interviewed by a psychiatrist or licensed clinical psychologist under proposed paragraph (e)(4)(ii) of this section. |

| | | |
|---|---|---|
| | | history evaluation is completed.<br><br>The proposed rule would not ~~would~~ establish employment history requirements for individuals whose UAA has been interrupted for 30 or fewer days. Proposed § 73.56(h)(3) would require the entities who are subject to this section to obtain and review a personal history disclosure from the applicant for UAA that would address the period since the individual's last period of UAA was terminated. However, the licensee, applicant, or C/V would be permitted to forego conducting an employment history evaluation for individuals whose UAA has been |
| | | interrupted for such a short period, because there would be little to be learned. |

| | | |
|---|---|---|
| (3) The licensee shall base its decision to grant, deny, revoke, or continue an unescorted access authorization on review and evaluation of all pertinent information developed. | (h)(8) Determination basis. The licensee's, applicant's, or C/V's reviewing official shall determine whether to grant, deny, unfavorably terminate, or maintain or amend an individual's unescorted access authorization status, based on an evaluation of all pertinent information that has been gathered about the individual as a result of any application for unescorted access authorization or developed during or following in any period during which the individual maintained unescorted access authorization. The licensee's, | Proposed § 73.56(h)(8) would amend but retain the meaning of current § 73.56(b)(3), which requires licensees to base a decision to grant, deny, revoke, or continue UAA on review and evaluation of all pertinent information developed. The terms used in the proposed paragraph, such as "unfavorably terminate" to replace "revoke" and "maintain" to replace "continue," would be updated for consistency with the terms currently used by the industry and in other portions of the proposed section. In addition, the proposed paragraph would include references to the reviewing official, rather than the licensee, to convey more |

| | | |
|---|---|---|
| | appendix A to this part. Footnote: 2. Notifications to the NRC for the declaration of an emergency class shall be performed in accordance with § 50.72 of this chapter. | especially if this event is the opening action on an ineffectively coordinated multiple-target attack. Such notice may permit other licensees to escalate to a higher protective level in advance of an attack. The Commission would expect licensees to notify the NRC Operations Center as soon as possible after they notify local law enforcement agencies, but within 15 minutes. The Commission may consider the applicability of this requirement to other types of licensees in future rulemaking. |

| | | |
|---|---|---|
| | | Footnote 1 would provide a cross reference to Appendix A to Part 73 which contains NRC contact information.<br><br>Footnote 2 would remind licensees of their concurrent emergency declaration responsibilities under 10 CFR 50.72. |
| | (a)(1) When making a report under paragraph (a) of this section, the licensees shall: | The proposed rule would include this introductory statement, which provides a structure for the following list of information to be provided in the 15-minute report. |
| | (a)(1)(i) Identify the facility name; and | This requirement would be added to ensure the licensee's facility is clearly identified when a report is made. |

| | | |
|---|---|---|
| Appendix B, Paragraph I.B.2.a. Individuals whose security tasks and job duties are directly associated with the effective implementation of the licensee physical security and contingency plans shall demonstrate mental alertness and the capability to exercise good judgment, implement instructions, assimilate assigned security tasks, and possess the acuity of senses and ability of expression sufficient to permit accurate communication by written, spoken, audible, visible, or other signals required by assigned job duties. | B.3.a. Armed and unarmed members of the security organization shall demonstrate the ability to apply good judgment, mental alertness, the capability to implement instructions and assigned tasks, and possess the acuity of senses and ability of expression sufficient to permit accurate communication by written, spoken, audible, visible, or other signals required by assigned duties and responsibilities. | This requirement to demonstrate good judgement, ability to implement instructions/tasks, and to communicate would be retained. The phrase "Individuals whose security tasks and job duties are directly associated with the effective implementation of the licensee physical security and contingency plans" would be replaced with the phrase "Armed and unarmed members of the security organization" to describe the requirement that these mental requirements are minimum standards that must apply to both armed and unarmed security personnel because they share similar duties and responsibilities for the physical protection of the site. |

| | | |
|---|---|---|
| Appendix B, Paragraph I.B.2.b. Armed individuals, and central alarm station operators, in addition to meeting the requirement stated in Paragraph a. above, shall have no emotional instability that would interfere with the effective performance of assigned security job duties. The determination shall be made by a licensed psychologist or psychiatrist, or physician, or other person professionally trained to identify emotional instability. | B.3.b. A licensed clinical psychologist, psychiatrist, or physician trained in part to identify emotional instability shall determine whether armed members of the security organization in addition to meeting the requirement stated in Paragraph a. of this section, have no emotional instability that would interfere with the effective performance of assigned duties and responsibilities. | The requirement regarding emotional instability would be retained. The phrase "Armed individuals, and central alarm station operators" would be replaced with the phrase "armed members of the security organization" for consistency with the terminology used in the proposed rule. |

alarm station operators

| | | |
|---|---|---|
| | | or intelligence gathering efforts. Events reported under paragraphs I or II would require a followup written report. Events reported pursuant to paragraph III would not require a followup written report. |
| | I. Events to be reported as soon as possible, but no later than 15 minutes after discovery, followed by a written report within sixty (60) days.<br><br>(a) The initiation of a security response consistent with a licensee's physical security plan, safeguards contingency plan, or defensive strategy based on actual or imminent threat against a nuclear power plant. | Paragraph I would be added to establish the types events to be reported within 15 minutes. Because the identification of information relating to an actual or potential threat could quickly result in an event, which may necessitate expedited Commission action (e.g., notification of other licensees or Federal authorities), a shortened reporting time would be required. This proposed requirement would also ensure that threat-related information would be made available to the Commission's threat assessment process |

| | | |
|---|---|---|
| | | in a timely manner. Initiation of response consistent with plans and the defensive strategy that are not related to an imminent or actual threat against the facility would not need to be reported (e.g false, or nuisance responses). Additional information regarding identification of events to be reported would be provided in guidance. |
| | I.(b) The licensee is not required to report security responses initiated as a result of information communicated to the licensee by the Commission, such as the threat warning system addressed in Appendix C to this part. | This provision would be added to reduce unnecessary regulatory burden on the licensees to notify the Commission of security responses initiated in response to communications from the Commission (e.g., changes to the threat level). |

| | | |
|---|---|---|
| I. Events to be reported within one hour of discovery, followed by a written report within 60 days. | II. Events to be reported within one (1) hour of discovery, followed by a written report within sixty (60) days. | This requirement would be retained and renumbered. |
| (a) Any event in which there is reason to believe that a person has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause: | II.(a) Any event in which there is reason to believe that a person has committed or caused, or attempted to commit or cause, or has made a threat to commit or cause: | This requirement would be retained with minor revision and renumbered. The term credible would be removed. The Commission's view is that a determination of the "credibility" of a threat is not a licensee responsibility, but rests with the Commission and the intelligence community. |
| (1) A theft or unlawful diversion of special nuclear material; or | II.(a)(1) A theft or unlawful diversion of special nuclear material; or | This requirement would be retained and renumbered. |

| | | |
|---|---|---|
| (2) Significant physical damage to a power reactor or any facility possessing SSNM or its equipment or carrier equipment transporting nuclear fuel or spent nuclear fuel, or to the nuclear fuel or spent nuclear fuel a facility or carrier possesses; or | II.(a)(2) Significant physical damage to any NRC-regulated power reactor or facility possessing strategic special nuclear material or to carrier equipment transporting nuclear fuel, or to the nuclear fuel or spent nuclear fuel facility which is possessed by a carrier; or<br>or spent nuclear fuel | This requirement would be retained with minor editorial changes to improve clarity and readability and renumbered. The phrase "NRC-regulated" would be added to specify that all Commission licensed facilities and transport would be covered by this requirement. This change would simplify the language in this section while retaining the basic requirement. |

| | | |
|---|---|---|
| (d) The actual or attempted introduction of contraband into a protected area, material access area, vital area, or transport. | II.(d) The actual or attempted introduction of contraband into any area or transport for which the licensee is required by Commission regulations to control access. | This requirement would be renumbered and revised to delete the previously specifically mentioned areas requiring access controls and change the language to include the actual or attempted entry of an unauthorized individual into any area or transport required to be controlled by Commission regulations (see considerations for paragraph II.(b) above). Additional information regarding identification of events to be reported will be provided in guidance. |

| | | |
|---|---|---|
| NRC Information Assessment Team (IAT) Advisories dated October 16, and November 15, 2001; May 20, 2003; March1, 2004; and October 5, 2005.<br><br>FBI's "Terrorist Threats to the U.S. Homeland: Reporting Guide for Critical and Key Resource Owners and Operators" dated January 24, 2005, (Official Use Only). | III. Events to be reported within four (4) hours of discovery. No written followup report is required.<br><br>(a) Any other information received by the licensee of suspicious surveillance activities, attempts at access, ~~or other information~~, including:<br><br>too open ended, need time operable, 4 hour provision<br><br>(1) Any security-related incident involving suspicious activity that may be indicative of potential pre-operational surveillance, reconnaissance, or intelligence-gathering activities directed against the facility. Such activity may include, but is not limited to, | This paragraph would add a requirement for power reactor licensees to report suspicious activities, attempts at access, etc., that may indicate pre-operational surveillance, reconnaissance, or intelligence gathering targeted against the facility. This change would more accurately reflect the current threat environment; would assist the Commission in evaluating threats to multiple licensees; and would assist the intelligence and homeland security communities in evaluating threats |

## V. Guidance

The NRC is preparing new regulatory guides that will contain detailed guidance on the implementation of the proposed rule requirements. These regulatory guides, currently under development, will consolidate and update or eliminate previous guidance that was used to develop, review, and approve the power reactor security plans that licensees revised in response to the post-September 11, 2001, security orders. Development of the regulatory guides is ongoing and the publication of the regulatory guides is planned after the publication of the final rule. Because this regulatory guidance may contain Safeguard Information (SGI) and/or classified information, these documents would only be available to those individuals with a need-to-know, and are qualified to have access to SGI and/or classified information, as applicable. However, the NRC ~~considers~~ has determined that access to these guidance documents is not necessary for the public or other stakeholders to provide informed comment on this proposed rule.

## VI. Criminal Penalties

For the purposes of Section 223 of the Atomic Energy Act, as amended, the Commission is proposing to amend 10 CFR Parts 50, 72, and 73 under Sections 161b, 161i, or 161o of the AEA. Criminal penalties, as they apply to regulations in Part 73, are discussed in § 73.81. The new §§ 73.18, 73.19, and 73.58 are issued under Sections 161b, 161i, or 161o of the AEA, and are not included in § 73.81(b).

## VII. Compatibility of Agreement State Regulations

Under the "Policy Statement on Adequacy and Compatibility of Agreement States Programs," approved by the Commission on June 20, 1997, and published in the Federal Register (62 FR 46517; September 3, 1997), this rule is classified as compatibility "NRC." Compatibility is not required for Category "NRC" regulations. The NRC program elements in this category are those that relate directly to areas of regulation reserved to the NRC by the AEA or the provisions of Title 10 of the Code of *Federal Regulations* (10 CFR), and although an Agreement State may not adopt program elements reserved to NRC, it may wish to inform its licensees of certain requirements via a mechanism that is consistent with the particular State's administrative procedure laws, but does not confer regulatory authority on the State.

## VIII. Availability of Documents.

The following table indicates which documents relating to this rulemaking are available to the public and how they may be obtained.

*Public Document Room (PDR).* The NRC's Public Document Room is located at the NRC's headquarters at 11555 Rockville Pike, Rockville, MD 20852.

Rulemaking Website (Web). The NRC's interactive rulemaking Website is located at http://ruleforum.llnl.gov. These documents may be viewed and downloaded electronically via this Website.

the terrorist attacks of September 11, 2001, based upon experience and insights gained by the Commission during implementation, (2) fulfill certain provisions of the Energy Policy Act of 2005, (3) add several new requirements that resulted from insights from implementation of the security orders, review of site security plans, and implementation of the enhanced baseline inspection program and force-on-force exercises, (4) update the regulatory framework in preparation for receiving license applications for new reactors, and (5) impose requirements to assess and manage site activities that can adversely affect safety and security. The proposed safety and security requirements would address, in part, a Petition for Rulemaking (PRM 50-80) that requested the establishment of regulations governing proposed changes to facilities which could adversely affect the protection against radiological sabotage.

The U.S. Nuclear Regulatory Commission is seeking public comment on the potential impact of the information collections contained in this proposed rule and on the following issues:

1. Is the proposed information collection necessary for the proper performance of the functions of the NRC, including whether the information will have practical utility?

2. Is the estimate of burden ~~accurate~~?

3. Is there a way to enhance the quality, utility, and clarity of the information to be collected?

4. How can the burden of the information collection be minimized, including the use of automated collection techniques?

A copy of the OMB clearance package may be viewed free of charge at the NRC Public Document Room, One White Flint North, 11555 Rockville Pike, Room O-1 F21, Rockville, MD 20852. The OMB clearance package and rule are available at the NRC worldwide Web site: http://www.nrc.gov/public-involve/doc-comment/omb/index.html for 60 days after the signature date of this notice and are also available at the rule forum site, http://ruleforum.llnl.gov.

Send comments on any aspect of these proposed information collections, including suggestions for reducing the burden and on the above issues, by (INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*) to the Records and FOIA/Privacy Services Branch (T-5 F52), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by Internet electronic mail to INFOCOLLECTS@NRC.GOV and to the Desk Officer, John A. Asalone, Office of Information and Regulatory Affairs, NEOB-10202, (3150-0002, 3150-0011, and 3150-new), Office of Management and Budget, Washington, DC 20503. Comments received after this date will be considered if it is practical to do so, but assurance of consideration cannot be given to comments received after this date. You may also e-mail comments to John_A._Asalone@omb.eop.gov or comment by telephone at (202) 395-4650.

## XIII. Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

(2) A hearing aid is acceptable provided suitable testing procedures demonstrate auditory acuity equivalent to the hearing requirement.

(3) The use of a hearing aid may not decrease the effective performance of the individual's assigned security job duties during normal or emergency operations.

d. Existing medical conditions.

(1) Individuals may not have an established medical history or medical diagnosis of existing medical conditions which could interfere with or prevent the individual from effectively performing assigned duties and responsibilities.

(2) If a medical condition exists, the individual shall provide medical evidence that the condition can be controlled with medical treatment in a manner which does not adversely affect the individual's fitness-for-duty, mental alertness, physical condition, or capability to otherwise effectively perform assigned duties and responsibilities.

e. Addiction. Individuals may not have any established medical history or medical diagnosis of habitual alcoholism or drug addiction, or, where this type of condition has existed, the individual shall provide certified documentation of having completed a rehabilitation program which would give a reasonable degree of confidence that the individual would be capable of effectively performing assigned duties and responsibilities.

f. Other physical requirements. An individual who has been incapacitated due to a serious illness, injury, disease, or operation, which could interfere with the effective

performance of assigned duties and responsibilities shall, before resumption of assigned duties and responsibilities, provide medical evidence of recovery and ability to perform these duties and responsibilities.

3. Psychological qualifications.

a. Armed and unarmed members of the security organization shall demonstrate the ability to apply good judgment, mental alertness, the capability to implement instructions and assigned tasks, and possess the acuity of senses and ability of expression sufficient to permit accurate communication by written, spoken, audible, visible, or other signals required by assigned duties and responsibilities.

alarm station operators +

b. A licensed clinical psychologist, psychiatrist, or physician trained in part to identify emotional instability shall determine whether armed members of the security organization in addition to meeting the requirement stated in paragraph a. of this section, have no emotional instability that would interfere with the effective performance of assigned duties and responsibilities.

c. A person professionally trained to identify emotional instability shall determine whether unarmed members of the security organization in addition to meeting the requirement stated in paragraph a. of this section, have no emotional instability that would interfere with the effective performance of assigned duties and responsibilities.

4. Medical examinations and physical fitness qualifications.

paragraphs II and IV of this appendix. Licensees shall make such reports to the Commission under the provisions of § 73.71 of this part.

I. Events to be reported as soon as possible, but no later than 15 minutes after discovery, followed by a written report within sixty (60) days.

(a) The initiation of a security response consistent with a licensee's physical security plan, safeguards contingency plan, or defensive strategy based on actual or imminent threat against a nuclear power plant.

(b) The licensee is not required to report security responses initiated as a result of information communicated to the licensee by the Commission, such as the threat warning system addressed in Appendix C to this part.

II. Events to be reported within one (1) hour of discovery, followed by a written report within sixty (60) days.

(a) Any event in which there is reason to believe that a person has committed or caused, or attempted to commit or cause, or has made a threat to commit or cause:

(1) A theft or unlawful diversion of special nuclear material; or

(2) Significant physical damage to any NRC-licensed power reactor or facility possessing strategic special nuclear material or to carrier equipment transporting nuclear fuel, or spent nuclear fuel or to the nuclear fuel or spent nuclear fuel facility which is possessed by a carrier; or

(3) Interruption of normal operation of any NRC licensed nuclear power reactor through the unauthorized use of or tampering with its components, or controls including the security system.

(b) An actual or attempted entry of an unauthorized person into any area or transport for which the licensee is required by Commission regulations to control access.

(c) Any failure, degradation, or the discovered vulnerability in a safeguard system that could allow unauthorized or undetected access to any area or transport for which the licensee is required by Commission regulations to control access and for which compensatory measures have not been employed.

(d) The actual or attempted introduction of contraband into any area or transport for which the licensee is required by Commission regulations to control access.

III. Events to be reported within four (4) hours of discovery. No written followup report is required.

(a) Any other information received by the licensee of suspicious surveillance activities, attempts at access, ~~or other information~~, including:

(1) Any security-related incident involving suspicious activity that may be indicative of potential pre-operational surveillance, reconnaissance, or intelligence-gathering activities directed against the facility. Such activity may include, but is not limited to, attempted surveillance or reconnaissance activity, elicitation of information from security or other site

quantities or greater of strategic special nuclear material, i.e., Category I SSNM facilities. Such facilities would include: production facilities, spent fuel reprocessing facilities, fuel processing facilities, and uranium enrichment facilities. The NRC plans to address separately whether the deployment of enhanced weapons is appropriate for other types of facilities, radioactive materials, or other property. Additionally, Section 651 of the EPAct 2005 requires the NRC to conduct security evaluations at selected licensed facilities, including periodic force-on-force exercises. That provision also requires the NRC to mitigate any potential conflict of interest that could influence the results of force-on-force exercises. These provisions would be reflected in proposed § 73.55.

### 1.3 Regulatory Objectives

The NRC has five objectives for the current rulemaking. The first objective is to make generically applicable security requirements imposed by Commission orders issued after the terrorist attacks of September 11, 2001, based upon experience and insights gained by the Commission during implementation.[1] The second objective is to fulfill certain provisions of the Energy Policy Act of 2005. The third objective is to add several new requirements that resulted from insights from implementation of the security orders, review of site security plans, and implementation of the enhanced baseline inspection program and force-on-force exercises. The fourth objective is to update the regulatory framework in preparation for receiving license applications for new reactors. The fifth objective is to impose requirements to assess and manage site activities that can adversely affect safety and security. The proposed safety and security requirements would address, in part, a Petition for Rulemaking (PRM 50-80) that requested the establishment of regulations governing proposed changes to facilities which could adversely affect the protection against radiological sabotage.

## 2. Identification and Preliminary Analysis of Alternative Approaches

This section presents preliminary analysis of the alternatives that the staff considered to meet the regulatory goals identified in the previous section. (Section 4 presents a more detailed analysis of the proposed rule option.) The staff considered two alternatives for revising Part 73's power plant security provisions as discussed below.

### 2.1 Option 1: No Action

Under Option 1, the no-action alternative, NRC would not amend the current regulations regarding power reactor security. Licensees would continue to comply with the Commission's security orders. This option would avoid certain costs that the proposed rule would impose. However, taking no action would not improve security measures as authorized by the EPAct 2005 or establish regulatory requirements for lessons learned. Additionally, taking no action would present a problem for establishing appropriate security measures for new reactors that did not receive orders.

---

[1] Specific details related to requirements that are Safeguards Information (SGI) will not be specified in regulations but will be available only to those with appropriate clearance and need to know.

### 2.2. Option 2: Amend Regulations to Enhance Power Reactor Security Operations

Under Option 2, NRC would conduct a rulemaking to address changes in several sections of 10 CFR Part 73 to enhance security operations at power reactors. These changes entail: (1) amending 10 CFR 73.2 to add definitions; (2) revising 10 CFR 73.55, 73.56, 73.71, Appendix B, Appendix C, and Appendix G; (3) adding 10 CFR 73.58 to introduce "safety/security interface" requirements, and (4) adding § 73.18, § 73.19, and Form 754 to implement EPAct 2005 provisions for background checks and authorization for use of enhanced weapons.

A comprehensive rulemaking would provide a means of addressing the identified issues and concerns with respect to Part 73. Through a comprehensive revision, the NRC could (1) ensure that all licensees would consistently implement measures to enhance security and safety at nuclear power plants; (2) modify current requirements to provide licensees with some flexibility; (3) address adjustments and changes in security plans that licensees have adopted through the development of the revised licensee security plans; (4) clarify the language of the rule; and (5) incorporate changes to address the requirements in the EPAct 2005

The NRC has estimated the benefits and costs of this option, as described in Sections 3 and 4 of this regulatory analysis, and has pursued Option 2 for the reasons discussed in Section 5.

## 3. Evaluation of Benefits and Costs

This section examines the benefits (values) and costs (impacts or burdens) expected to result from this rulemaking, and is presented in two subsections. Section 3.1 identifies attributes that are expected to be affected by the rulemaking. Section 3.2 describes how benefits and costs have been analyzed.

### 3.1 Identification of Affected Attributes

This section identifies the factors within the public and private sectors that the regulatory alternatives (discussed in Section 2) are expected to affect. These factors are classified as "attributes" using the list of potential attributes provided by NRC in Chapter 5 of its *Regulatory Analysis Technical Evaluation Handbook.*[2] Affected attributes include the following:

- Safeguards and Security Considerations – The proposed actions are intended to establish requirements that will provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public heath and safety.
- Industry Implementation – The proposed action would require licensees to make facility modifications and to revise their

[2] *Regulatory Analysis Technical Evaluation Handbook, Final Report*, NUREG/BR-0184, Office of Nuclear Regulatory Research, January 1997.

defend against the DBT. There would also be a reduced risk that public health and occupational health will be affected by radiological releases resulting from radiological sabotage. The proposed rule would also reduce the risk that off-site and on-site property will be affected by radiological releases resulting from radiological sabotage.

The new requirements in the rule are expected to result in specific qualitative benefits listed below:

- The security plan updates and revisions that would be required by the proposed rule would lead to the consistent implementation of best security practices.

- Current security regulations do not contain requirements related to cyber security. The NRC issued orders after September 11, 2001, that required power reactor licensees to implement interim compensatory measures to enhance cyber security licensees. These security measures required an assessment sufficient to provide protection against the cyber threats at the time of the orders. However, as licensees implement digital upgrades for many systems at their plants the potential for cyber threats will be increased. The proposed requirements would maintain the intent of the security orders by establishing the requirement for a cyber security program to protect any systems that can, if compromised, adversely impact safety, security or emergency preparedness.

- The proposed rule would ensure that escorts are trained and knowledgeable about their duties while accompanying visitors. This proposed requirement would reduce the risk of a security incident initiated by a visitor since escorts would be better informed regarding visitor's authorized activities.

- Current regulatory requirements ensure that both CAS and SAS have equivalent alarm annunciation and communication capabilities, but do not explicitly require equivalent assessment, monitoring, observation, and surveillance capabilities. Further, the current requirement of 73.55(e)(1) states "All alarms required pursuant to this part must annunciate in a continuously manned central alarm station located within the protected area and in at least one other continuously manned station not necessarily onsite, so that a single act cannot remove the capability of calling for assistance or otherwise responding to an alarm." The Commission orders added enhanced detection and assessment capabilities, but did not require equivalent capabilities for both CAS and SAS. The security plans approved by the Commission on October 29, 2004, varied, due to the performance-based nature of the requirements, with respect to how the individual licensees implemented these requirements, but all sites were required to provide CAS and SAS with functionally equivalent capabilities to support the implementation of the site protective strategy.

  The proposed rule extends the requirement for no single act to remove capabilities to the key functions required of the alarm stations and would require licensees to implement protective measures such that a single act would not disable the intrusion detection, assessment, and communications capabilities of both the CAS and SAS. This proposed requirement would ensure continuity of response operations during a security event by ensuring that the detection, assessment, and communications

functions required to effectively implement the licensee's protective strategy are maintained despite the loss of one or the other alarm station. For the purposes of assessing the regulatory burden of this proposed rule, the NRC assumed that all licensees would require assessments and approximately one third of the licensees would choose to implement hardware modifications.

The NRC has concluded that protecting the alarm stations such that a single act does not disable the key functions would provide an enhanced level of assurance that a licensee can maintain detection, assessment and communications capabilities required to protect the facility against the design basis threat of radiological sabotage. For new reactor licensees, licensed after the publication of this rule, the Commission would require CAS and SAS to be designed, constructed, and equipped with equivalent standards.

- Current regulatory requirements require back-up power for alarm annunciation and non-portable communication equipment, but do not require uninterruptible back-up power. Although not specifically required, many licensees have installed uninterruptible power to their security systems for added reliability of these electronic systems. However, the Commission has not required uninterruptible power for assessment systems. Uninterruptible back-up power would provide an enhanced level of assurance that a licensee can maintain detection, assessment and communication capabilities required to defend the facility against the design basis threat. This new requirement would reduce the risk of losing detection, assessment, and communication capabilities during a loss of the normal power supply.

- Current regulatory requirements address the use of closed circuit television systems, but do not explicitly require them. Although not specifically required, all licensees have adopted the use of video surveillance in their site security plans, and many of the licensees have adopted advanced video surveillance technology to provide real-time and play-back/recorded video images to help security officials determine the cause of an alarm annunciation. Advanced video technology would provide an enhanced level of assurance that a licensee can assess the cause of an alarm annunciation and initiate a timely response capable of defending the facility against the threat up to and including the design basis threat.

- The proposed safety-security interface requirements would reduce the risk of adverse safety-security interactions. These requirements would enhance the communication among nuclear power plant staff in order to avoid adverse safety or security effects.

- The proposed rule contains several new reporting provisions. It would require licensees to notify the NRC Operations Center no later than 15 minutes after discovery of an actual or imminent threat against the facility including a requirement to follow this report with a written report within 60 days. Additionally, the proposed rule would require licensees to report within 4 hours to NRC incidents of suspicious activity or tampering. These proposed requirements enable NRC to quickly obtain information that could

exercises and to mitigate any potential conflict of interest that could influence the results of force-on-force exercises. These provisions of EPAct 2005 would be incorporated into the newly proposed §§ 73.18 and 73.19, and the revision to proposed 73.55 and the newly proposed NRC Form 754 (Enclosure 2). To implement the EPAct 2005 provisions efficiently, the NRC expanded the rulemaking's scope beyond power reactors (for the EPAct 2005 provisions related to the use of enhanced weapons and firearms background checks only) to cover facilities authorized to possess formula quantities or greater of strategic special nuclear material (i.e., Category I SSNM facilities). Such facilities would include: production facilities, spent fuel reprocessing facilities, fuel processing facilities, and uranium enrichment facilities.

Through implementing the security orders, reviewing the revised site security plans, and evaluating force-on-force exercises, the NRC has identified some additional security measures necessary to ensure that licensees provide high assurance that public health and safety and the common defense and security are adequately protected.

Finally, Petition for Rulemaking (PRM 50-80), requested the establishment of regulations governing proposed changes to facilities which could adversely affect their protection against radiological sabotage. This petition was partially granted and the proposed new § 73.58 contains requirements to address this area.

The proposed amendments to the physical security requirements for power reactors, and for the new weapons requirements, Category I SSNM facilities, would result in changes to the following existing sections and appendices in 10 CFR Part 73:

- 10 CFR 73.2, Definitions.
- 10 CFR 73.55, Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.
- 10 CFR 73.56, Personnel access authorization requirements for nuclear power plants.
- 10 CFR 73.71, Reporting of safeguards events.

- 10 CFR 73, Appendix B, General criteria for security personnel.
- 10 CFR 73, Appendix C, Licensee safeguards contingency plans.
- 10 CFR 73, Appendix G, Reportable safeguards events.

The proposed amendments would also add three new sections to Part 73:

- Proposed § 73.18, Firearms background checks for armed security personnel.
- Proposed § 73.19, Authorization for use of enhanced weapons.
- Proposed § 73.58, Safety/security interface requirements for nuclear power reactors.

The proposed rule would also add a new NRC Form 754 under the proposed new § 73.18.

Conforming changes to the requirements listed below are proposed in order to ensure that cross-referencing between the various security regulations in Part 73 are preserved, and to avoid revising requirements for licensees who are not within the scope of this proposed rule. The following requirements contain conforming changes:

- Section 50.34, "Contents of applications; technical information" would be revised to align the application requirements with the proposed revisions to Appendix C to 10 CFR Part 73.

- Section 50.54, "Conditions of licenses" would be revised to conform with the proposed revisions to sections in Appendix C to 10 CFR Part 73.

- Section 50.72, "Immediate notification requirements for operating nuclear power reactors" would be revised to state (in footnote 1) that immediate notification to the NRC may be required (per the proposed § 73.71 requirements) prior to the notification requirements under the current § 50.72.

concluded that there will be no significant radiological environmental impacts associated with implementation of the proposed rule requirements for the following reasons:

(1) The proposed revision to the Part 73 security requirements would not result in changes to the design basis requirements for the structures, systems, and components (SSCs) in the facility that function to limit the release of radiological effluents during and following postulated accidents. As a result, all the SSCs associated with limiting the releases of offsite radiological effluents would continue to be able to perform their functions, and as a result, there would be no significant radiological effluent impact. In this regard, the safety-security requirement (new section added as § 73.58) is intended to address the interface between security and safety, and the need to ensure that the potential for adverse effects on safety (due to security actions) or security (due to safety actions) are assessed and managed such that facility safety and security is maintained.

(2) The standards and requirements applicable to radiological releases and effluents would not be affected by this rulemaking and would continue to apply to the SSCs affected by this rulemaking.

The principal effect of this action would be to revise the governing regulations pertaining to security to make them more closely align with the previously imposed orders, to make changes required to implement the EPAct 2005, and to add several new requirements. The majority of these requirements stem from the security orders issued after September 11, 2001, and are already in place at power reactors. None of the proposed revisions have an impact on occupational exposures, consequently the NRC has concluded that this action would cause no impact on occupational exposure.

For the reasons discussed above, the action will not significantly increase the probability or consequences of accidents, nor result in changes being made in the types of any effluents that may be released off-site, and there would be no significant increase in occupational or public radiation exposure.

With regard to potential nonradiological impacts, implementation of the rule requirements would have no impact on the environment. The revised requirements would not affect any historic sites, would not affect nonradiological plant effluents, and would have no other environmental impact. Therefore, there would be no significant nonradiological environmental impacts associated with the action.

Accordingly, the NRC staff concludes that there would be no significant environmental impacts associated with the action.

Alternatives to the Proposed Action:

As an alternative to the rulemakings described above, the NRC staff considered not taking the action (i.e., the "no-action" alternative). Not revising the security regulations would result in no change in current environmental impacts since the proposed requirements have no environmental impact and taking no action therefore results in no net change to the environment. However, the no action alternative would leave the governing security regulations as they are, and the regulation would not reflect the actual requirements governing security. In addition, not taking action would cause the NRC to not be responsive to the EPAct 2005. The NRC staff concluded that leaving the governing security regulations unaligned with order requirements is not a desirable regulatory practice . The Commission has directed the staff to revise the regulations in a Staff Requirements Memorandum dated August 23, 2004. Finally, the no action alternative would not be implement the requirements in the EPAct 2005.

redundant ?

NOTATION VOTE

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: COMMISSIONER MERRIFIELD

SUBJECT: **SECY-06-0126 - PROPOSED RULEMAKING - POWER REACTOR SECURITY REQUIREMENTS (RIN 3150-AG63)**

Approved __X__ Disapproved _____ Abstain _____

Not Participating _____

COMMENTS:

Approved, subject to the attached comments.

SIGNATURE

6/28/06
DATE

Entered on "STARS" Yes X No ___

## Commissioner Merrifield's Comments on SECY-06-0126

### Proposed Rulemaking - Power Reactor Security Requirements

I approve the staff recommendation to publish the proposed amendments to 10 CFR Parts 50, 72, and 73, and appendices, in the Federal Register for public comment, subject to the attached edits. This comprehensive rulemaking will codify the requirements imposed on nuclear power plant licensees through Commission Orders, and bring closure to the significant nuclear power plant security issues raised by the terrorist attacks of September 11, 2001. In addition, the proposed rule incorporates provisions that Congress enacted through the 2005 Energy Policy Act legislation.

While I am not enamored of rule packages on the order of one thousand pages, I believe in this case the volume is justified. The associated tables included in this rule package provide section-by-section explanations of the proposed changes that offer stakeholders without security clearances a chance to understand how the staff arrived at the proposed changes in a way that does not compromise common defense and security. I commend the staff for discussing the proposed changes in an open manner that allows meaningful public comment on security requirements at nuclear power plants.

I note the staff plans to conduct a public meeting during the public comment period. This is a good first step, but based on the sheer volume of issues being addressed, more than one public meeting may be needed to ensure that the staff provides stakeholders a chance to understand the reasoning behind the proposed changes. Recent experience with other voluminous rule packages leads me to believe that perhaps a second, or even a third, public meeting may necessary to fully vet the issues addressed in this proposed rule.

| PROPOSED LANGUAGE | CONSIDERATIONS |
| --- | --- |
| § 73.19(d) *Approval process.*<br>(1) *Commission approval.* (i) Licensees and certificate holders specified in paragraph (b) of this section who choose to utilize enhanced weapons as part of their physical protection program, shall submit to the Commission for prior review and written approval, new or revised physical security plans, training and qualification plans, safeguards contingency plans, and a safety assessment incorporating the use of the specific enhanced weapons the licensee or certificate holder intends to use. Licensees or certificate holders shall submit such revised plans for prior Commission review and written approval notwithstanding the provisions of §§ 50.54(p), 70.32(e), and 76.60 of this chapter. | This paragraph would describe the process for Commission approval of a licensees or certificate holders plans to use enhanced weapons. The use of such weapons would be incorporated into security plans for prior Commission review and approval. This paragraph would also require the submission of a new safety assessment evaluation of the onsite and offsite impacts from the use of the enhanced weapons (in protecting the facility or from training activities). Submission of such revised plans for prior review and approval would be required irrespective of whether the licensee or certificate holder concludes the use of these enhanced weapons would not cause "a decrease in security effectiveness." |

| PROPOSED LANGUAGE | CONSIDERATIONS |
| --- | --- |
| § 73.19(d)(1)(ii) ~~These plans~~, in addition to other requirements ~~for these plans~~ set forth in this part, ~~must address the following issues~~ – (A) Specific types or models, calibers, and numbers of enhanced weapons to be used; (B) Tactical approaches and personnel to be employed in using these enhanced weapons; (C) Assessment of any potential safety impact on the facility or radioactive material from the use of these enhanced weapons; (D) Assessment of any potential safety impact on public or private facilities, public or private property, or on members of the public in areas outside of the site boundary from the use of these enhanced weapons; and | This paragraph would require additional specific information to be included in the new or updated physical security plans, training and qualification plans, and safeguards contingency plans provided to the Commission for review and approval. Tactical approaches would include the personnel and methods used to employ these weapons, including areas or locations where enhanced weapons could be employed or areas where their use may be limited (e.g., safety issues associated with a specific area of the facility). This paragraph would require an assessment of the onsite and offsite safety impacts from the use of the enhanced weapons to protect the facility. |
| § 73.19(d)(1)(ii)(E) Assessment of any potential safety impact on public or private facilities, public or private property, or on members of the public from the use of these enhanced weapons at training facilities intended for proficiency demonstration and qualification purposes. | See considerations for § 73.19(d)(1) above. |

would be added

| PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|
| § 73.2 Definitions. | ~~Would add~~ three new definitions to this section as conforming changes to the new §§ 73.18 and 73.19 for *covered weapon*, *enhanced weapon*, and *standard weapon*. Other new definitions that would added as conforming changes to this section in support of other regulations (e.g., *safety/security interface* and *target set*) are discussed in other Tables under this notice. |
| *Covered weapon* means any handgun, rifle, shotgun, short-barreled shotgun, short-barreled rifle, semi-automatic assault weapon, machine gun, ammunition for any such gun or weapon, or a large capacity ammunition feeding device as specified under § 161A of the Atomic Energy Act of 1954, as amended. Covered weapons includes both enhanced weapons and standard weapons; however, enhanced weapons do not include standard weapons.<br>*Enhanced weapon* means any short-barreled shotgun, short-barreled rifle, semi-automatic assault weapon, machine gun, or a large capacity ammunition feeding device. Enhanced weapons do not include destructive devices, including explosives or weapons greater than 50 caliber (i.e., greater than a 1.27 cm [0.5 in] diameter bore).<br>*Standard weapon* means any handgun, rifle, or shotgun. | A definition for *covered weapon* would be used as an overall term to encompass the weapons and devices listed in Sec. 161A. of the AEA. The definitions of the specific firearms, ammunition, or devices within this term would be the same as those found in ATF's regulations in 27 CFR Part 478, Subpart B as of September 11, 2005.<br>Definitions for *enhanced weapon* and *standard weapon* would also be added to support the differing scope of these new sections (e.g., a licensee's current authority to possess handguns, shotguns, and rifles under State law is not obviated by Sec. 161A). The relationship between covered weapon, enhanced weapon, and standard weapon would be explained. Also, enhanced weapons would not include destructive devices as defined under ATF's regulations. The NRC's authority under Sec. 161A does not include destructive devices. |

Table 2 - Part 73 Section 73.55

Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

| CURRENT LANGUAGE | PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|---|
| Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage. | Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage. | This title would be retained. |
| | (a) Introduction. | This header would be added for formatting purposes. |
| § 73.55 By Dec. 2, 1986, each licensee, as appropriate, shall submit proposed amendments to its security plan which define how the amended requirements of Paragraphs (a), (d)(7), (d)(9), and (e)(1) will be met. | (a)(1) By **[insert date - 180 days - after the effective date of the final rule published in the *Federal Register*]**, each nuclear power reactor licensee, licensed under 10 CFR Part 50, shall incorporate the revised requirements of this section through amendments to its Commission approved Physical Security Plan, Training and Qualification Plan, and Safeguards Contingency Plan, referred to collectively as "approved security plans," and shall submit the amended security plans to the | This requirement would be added to discuss the types of Commission licensees to whom the proposed requirements of this section would apply and the schedule for submitting the amended security plans. The Commission intends to delete the current language, because it applies only to a past rule change that is completed. The proposed requirements of this section would be applicable to decommissioned/ing reactors unless otherwise approved by the Commission. |
| | Commission for review and approval. | |

GENERIC COMMENT: hyphenate

## Table 2 - Part 73 Section 73.55

Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

| CURRENT LANGUAGE | PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|---|
| 73.55(b)(1)(i) The licensee is responsible to the Commission for maintaining safeguards in accordance with Commission regulations and the licensee's security plan. | (a)(4) The licensee is responsible ~~to the Commission~~ for maintaining the onsite physical protection program in accordance with Commission regulations and related Commission-directed orders through the implementation of the approved security plans and site implementing procedures. | This requirement would retain the current requirement that the licensee is responsible for meeting Commission regulations and the approved security plans. The phrase "through the implementation of the approved security plans and site implementing procedures" would be added to describe the relationship between Commission regulations, the approved security plans, and implementing procedures. The word "safeguards" would be replaced with the phrase "physical protection program" to |

Table 2 - Part 73 Section 73.55

Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

| CURRENT LANGUAGE | PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|---|
| | | elements would comprise the component actions of response and would be provided by personnel trained and equipped in accordance with a response strategy. The third element "Intercept" would be the act of placing a person at an intersecting defensive position directly in the path of advancement taken by the threat, and between the threat and the protected target or target set element. The fourth element "Challenge" would be to verbally or physically confront the threat to impede, halt, or otherwise interact with |

Table 2 - Part 73 Section 73.55

Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

| CURRENT LANGUAGE | PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|---|
| | | prevention of significant core damage and spent fuel sabotage ~~is~~ are measurable performance criteria against which the Commission would evaluate the effectiveness of the licensee physical protection program. The phrase "as bounded by the design basis threat" would be used to clarify the Commission's view that the license must ensure that the physical protection program is designed to protect against the design basis threat and all other threats that do not rise to the level of the design basis threat. The |

Table 2 - Part 73 Section 73.55

Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

| CURRENT LANGUAGE | PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|---|
| § 73.55(b)(4)(i) Upon the request of an authorized representative of the Commission, the licensee shall demonstrate the ability of the physical security personnel to carry out their assigned duties and responsibilities. | (b)(5) Upon the request of an authorized representative of the Commission, the licensee shall demonstrate the ability to meet Commission requirements through the implementation ~~of any component~~ of the physical protection program, ~~to~~ including ~~but not limited to~~ the ability of armed and unarmed personnel to perform assigned duties and responsibilities required by the approved security plans and licensee procedures. | This requirement would retain the current requirement for demonstration and would contain minor revisions to apply this requirement to the licensee's ability to implement the physical protection program and not be limited to only the ability of security personnel to carry out their duties. This proposed requirement would clarify the Commission's view that the licensee must also demonstrate the effectiveness of plans, procedures, and equipment to accomplish their intended function within the physical protection program. |

Table 2 - Part 73 Section 73.55

Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

| CURRENT LANGUAGE | PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|---|
| | (b)(6) The licensee shall establish and maintain a written performance evaluation program in accordance with appendix B and appendix C to this part, to demonstrate and assess the effectiveness of armed responders and armed security officers to perform their assigned duties and responsibilities ~~required for the protection of~~ to target sets described in paragraph (f) and appendix C to this part, through implementation of the licensee protective strategy. | This requirement would be added to specify that this performance evaluation program would be the mechanism by which the licensee would demonstrate the capabilities described by the performance based requirements of the proposed paragraphs (b)(2) through (4). The word "target sets" would be used consistent with the proposed (b)(3) to describe the combination of equipment and operator actions which, if all are prevented from performing their intended safety function or prevented from being accomplished, |

Table 2 - Part 73 Section 73.55

Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

| CURRENT LANGUAGE | PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|---|
| | (c)(1)(ii) Site-specific conditions that affect implementation of Commission requirements. | This requirement would be added to reflect the Commission's view that licensees must focus attention on site-specific conditions in the development and implementation of site plans, procedures, processes, response strategies, and ultimately, the licensee capability to achieve the performance objective of the proposed (b)(1). |
| | (c)(2) Protection of security plans. The licensee shall protect the approved security plans and other related safeguards information against unauthorized disclosure in accordance with the requirements of § 73.21. | This requirement would be added to emphasize the requirements for the protection of safeguards information in accordance with the requirements of § 73.21. |
| | (c)(3) Physical Security Plan. | This header would be added for formatting purposes. |

Table 2 - Part 73 Section 73.55

Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

| CURRENT LANGUAGE | PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|---|
| § 73.55(b)(4)(ii) Each licensee shall establish, maintain, and follow an NRC-approved training and qualifications plan ... | (c)(4)(i) The licensee shall establish, maintain, and follow a Commission-approved training and qualification plan, that describes how the criteria set forth in appendix B "General Criteria for Security Personnel," to this part will be implemented. | This requirement would retain and separate two current requirements of § 73.55(b)(4)(ii). This proposed requirement would require the licensee to provide a training and qualification plan. |
| § 73.55(b)(4)(ii) ...outlining the processes by which guards, watchmen, armed response persons, and other members of the security organization will be selected, trained, equipped, tested, and qualified to ensure that these individuals meet the requirements of this paragraph. | (c)(4)(ii) The training and qualification plan must describe the process by which armed and unarmed security personnel, watchpersons, and other members of the security organization will be selected, trained, equipped, tested, qualified, and re-qualified to ensure that these individuals possess and maintain the knowledge, skills, and abilities required to carry out their assigned duties and responsibilities effectively. | This requirement would retain the requirement for the licensee to outline ~~this~~ the processes in this plan with minor revisions. The phrase "guards, watchmen, armed response persons" would be replaced by the phrase "armed and unarmed security personnel, watchpersons" to generically identify all members of the security organization. The Commission does not intend that administrative staff be included except as these personnel would be used to perform duties required to detect, assess, |

Table 2 - Part 73 Section 73.55

Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

| CURRENT LANGUAGE | PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|---|
| § 73.55(b)(3) The licensee shall have a management system to provide for... | (c)(6)(iv) The licensee shall: would | This requirement would be retain and separate the two current requirements of § 73.55(b)(3) with minor revisions. The phrase "management system" would be replaced with the word "process." The current requirement to have a management system would be addressed in the proposed § 73.55(d)(2). |
| § 73.55(b)(3) ...the development, revision, implementation, and enforcement of security procedures. | (c)(6)(iv)(A) Develop, maintain, enforce, review, and revise security implementing procedures. | This requirement would retain the requirement to develop, revise, implement, and enforce security procedures. The words "maintenance and review" would be added to clarify these tasks as necessary functions. The word "implementation" would be deleted because implementation is addressed in the proposed (c)(6)(i) through (iii). |

Table 2 - Part 73 Section 73.55

Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

| CURRENT LANGUAGE | PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|---|
| § 73.55(b)(3)(ii) Provision for written approval of these procedures and any revisions to the procedures by the individual with overall responsibility for the security functions. | (c)(6)(iv)(B) Provide a process for the written approval of implementing procedures and revisions by the individual with overall responsibility for the security functions. | This requirement would retain the current requirement for written approval with minor revisions. |
| | (c)(6)(iv)(C) Ensure that changes made to implementing procedures do not decrease the effectiveness of any procedure to implement and satisfy Commission requirements. | This requirement would be added to ensure that the licensee process for making changes to implementing procedures includes a process to ensure that changes do not result in a reduction of effectiveness or result in a conflict with other site procedures. |

Table 2 - Part 73 Section 73.55

Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

| CURRENT LANGUAGE | PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|---|
| 73.55(b)(2) At least one full time member of the security organization who has the authority to direct the physical protection activities of the security organization shall be onsite at all times. | (d)(2)(ii) At least one member, onsite and available at all times, who has the authority to direct the activities of the security organization and who is assigned no other duties that would interfere with this individual's ability to perform these duties in accordance with the approved security plans and licensee protective strategy. | This requirement would be retained with minor revisions. The phrase "who is assigned no other duties which would interfere with" would be added to ensure that the designated individual would not be assigned any duties that would prevent or interfere with the ability to direct these activities when needed. |
| § 73.55(b)(4)(i) The licensee may not permit an individual to act as a guard, watchman, armed response person, or other member of the security organization unless the individual has been trained, equipped, and qualified to perform each assigned security job duty in accordance with Appendix B, "General Criteria for Security Personnel," to this part. | (d)(3) The licensee may not permit any individual to act as a member of the security organization unless the individual has been trained, equipped, and qualified to perform assigned duties and responsibilities in accordance with the requirements of appendix B (to this part) and the Commission-approved training and qualification plan. | This requirement would be retained with minor revisions. |

Table 2 - Part 73 Section 73.55

Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

| CURRENT LANGUAGE | PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|---|
| § 73.55(b)(1)(ii) The NRC may inspect, copy, and take away copies of all reports and documents required to be kept by Commission regulations, orders, or applicable license conditions whether the reports and documents are kept by the licensee or the contractor. | (d)(5)(ii) The Commission may inspect, copy, retain, and remove all reports and documents required to be kept by Commission regulations, orders, or applicable license conditions whether the reports and documents are kept by the licensee or the contractor. contractor security employee | This requirement would be retained with minor revisions. |
| | (d)(5)(iii) ~~An individual~~ may not be assigned to any position involving detection, assessment, or response to unauthorized activities unless that individual has satisfied the requirements of § 73.56. | This requirement would be added for consistency with the proposed requirements of the proposed (d)(4). This proposed requirement would be stipulated in a contract because it relates to a function of the contract. |

Table 2 - Part 73 Section 73.55

Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

| CURRENT LANGUAGE | PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|---|
| § 73.55(b)(1)(iv) The contractor will not assign any personnel to the site who have not first been made aware of these responsibilities.<br>§ 73.55(b)(4)(i) The licensee may not permit an individual an individual to act as a guard, watchman, armed response person, or other member of the security organization unless the individual has been trained, equipped, and qualified to perform each assigned security job duty in accordance with Appendix B... | (d)(5)(iv) A ~~individual~~ contractor security employee may not be assigned duties and responsibilities required to implement the approved security plans or licensee protective strategy unless that individual has been properly trained, equipped, and qualified to perform their assigned duties and responsibilities in accordance with appendix B and the Commission-approved training and qualification plan. | This requirement would retain and combine two current requirements of § 73.55(b)(1)(iv) and § 73.55(b)(4)(i) with minor revisions necessary for consistency with the proposed rule. |

Table 2 - Part 73 Section 73.55

Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

| CURRENT LANGUAGE | PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|---|
| § 73.55(c) Physical barriers. | (e) Physical Barriers. Based upon the licensee's protective strategy, analyses, and site conditions that affect the use and placement of physical barriers, the licensee shall install and maintain physical barriers that are designed and constructed as necessary to deter, delay, and prevent the introduction of unauthorized personnel, vehicles, or materials into areas for which access must be controlled or restricted. | This requirement would be added to provide a performance based requirement for determining the use and placement of physical barriers required for protection of personnel, equipment, and systems the failure of which could directly or indirectly endanger public health and safety. The phrase "Based upon the licensee protective strategy, analyses, and site specific conditions", would be used to ensure that licensees consider protective strategy requirements and needs, as well as any analyses conducted by the |

Table 2 - Part 73 Section 73.55

Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

| CURRENT LANGUAGE | PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|---|
| 73.55(e)(3) All emergency exits in each protected area and each vital area shall be alarmed. | (e)(6)(iii) All emergency exits in the protected area must be secured by locking devices that allow exit only, and alarmed. | This requirement would retain and separate the two current requirements with minor revision. The phrase "secured by locking devices which allow exit only" would be added to provide a performance based requirement relative to the function of locking devices with emergency exit design to prevent entry. Vital areas would be addressed in the proposed § 73.55(e)(6)(vii). be |
| | (e)(6)(iv) Where building walls, roofs, or penetrations comprise a portion of the protected area perimeter barrier, an isolation zone is not necessary, provided that the detection, assessment, observation, monitoring, and surveillance requirements of this section are met, appropriately designed and constructed barriers are installed, and the area is described in the approved security plans. | This requirement would added to provide a performance based requirement for instances where this site condition would exist. |

Table 2 - Part 73 Section 73.55

Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

| CURRENT LANGUAGE | PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|---|
| | (m)(1)(i) The licensee shall describe the cyber-security program requirements in the approved security plans. | This requirement would be added to ensure licensees to have a comprehensive security plan by integrating cyber-security into the overall onsite physical protection program. As licensees take advantage of computer technology to maximize plant productivity, the role of computer systems at nuclear power plants is increasing, the Commission has determined that incorporation of a cyber-security program into the Commission approved security plans would be a prudent and necessary security enhancement. |

Table 2 - Part 73 Section 73.55

Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

| CURRENT LANGUAGE | PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|---|
| | (m)(3)(i) The licensee shall apply cyber-security requirements and policies that identify management expectations and requirements for the protection of computer systems. | This requirement would be added to create a computer security program that establishes specific goals and assigns responsibilities to employees to meet those goals. |
| | (m)(3) (ii) The licensee shall develop and maintain implementing procedures to ensure cyber-security requirements and policies are implemented effectively. | This requirement be added to ensure the licensee develops, implements, and enforces, detailed guidance documents that licencee employees would be required to follow to meet the stated security goals. |
| | (m)(4) Incident Response and Recovery. | This header would be added for formatting purposes. |

Table 2 - Part 73 Section 73.55

Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

| CURRENT LANGUAGE | PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|---|
| § 73.55(g)(4) These reports must be maintained in an auditable form, available for inspection, for a period of 3 years. | (r)(2) The licensee shall maintain all records required to be kept by Commission regulations, orders, or license conditions, as a record until the Commission terminates the license for which the records were developed and shall maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified by the Commission. | This requirement would be retained and revised to consolidate multiple current records retention requirements rather than state the same requirement multiple times for each record throughout this rule. The phrase "unless otherwise specified by the Commission" would be used address any conflict that may arise between other records retention requirements such that the more restrictive requirement would take precedence. |
| | (s) Safety/Security Interface. In accordance with the requirements of § 73.58, the licensee shall develop and implement a process to inform and coordinate safety and security activities to ensure that these activities do not adversely affect the capabilities of the security organization to satisfy the requirements of this section, or overall plant safety. | This requirement would be added to provide specific reference to the proposed § 73.58 for Safety and Security Interface requirements |

Table 4 - Proposed Part 73 Section 73.58

Safety/security interface.

| PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|
| | The Commission has determined that the proposed safety/security rule requirements are necessary for reasonable assurance that the public health and safety, and common defense and security continue to be adequately protected because the current regulations do not specifically require evaluation of the effects of plant changes on security or the effects of security plan changes on plant safety. Further, the regulations do not require communication about the implementation and timing of changes, which would promote awareness of the effects of changing conditions, and result in appropriate assessment and response. |

NOTATION VOTE

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: **COMMISSIONER JACZKO**

SUBJECT: **SECY-06-0126 - PROPOSED RULEMAKING - POWER REACTOR SECURITY REQUIREMENTS (RIN 3150-AG63)**

Approved ___X___ Disapproved _____ Abstain _____

Not Participating _____

COMMENTS: **See attached comments.**

SIGNATURE

1/27/06

DATE

Entered on "STARS" Yes X No ___

**Commissioner Jaczko's Comments on SECY-06-0126**
**Proposed Rulemaking - Power Reactor Security Requirements**

I approve of the staff's proposal to publish the proposed rule for public comment and complete the rulemaking within a schedule of one year. This rulemaking, which in large part codifies and improves the many of the elements of security orders imposed on power reactor licensees since September 11, 2001 and implements certain provisions of the Energy Policy Act of 2005, is very important step toward addressing security concerns following September 11 and preparing for potential new reactor licensing. I commend Chairman Diaz, Commissioner McGaffigan, Commissioner Merrifield for their leadership on the post-September 11 security work and the staff for their commitment to preparing such a comprehensive and ever-changing proposal on such a tight schedule.

Despite the importance of this proposed rule, I do not view this rulemaking by itself as the most important security rulemaking in process. This rulemaking is one of three security rulemakings focused on the security of power reactors the Commission is working on. The others are the on-going rulemaking on the design basis threat and the planned rulemaking on security assessments for new reactor designs

Most of the requirements set forth in this rulemaking are already in place as a result of the various security orders issued since September 11, 2001, and this rule change will primarily add stability and finality to that process. What remains undone, however, is an important rulemaking to require applicants for combined operating licenses of new reactors to design security features into their future facilities.

Today's regulatory framework, embodied in this rulemaking and imposed by the post-September 11 security orders, relies heavily on maintaining a physical security program to protect vital areas of a plant and on mitigating strategies to ameliorate the effects of losses of large areas of the facility of due to fires and explosions. It is imperative that future designs become inherently safer and more secure through design features that reduce the need for physical security programs, potentially reducing the number of needed armed responders, and through design features that prevent the loss of safety systems and functions, eliminating the need for mitigating strategies. The security assessment rulemaking needs to address these important issues. Completing this rulemakings in a timely manner will be crucial to finalizing a robust regulatory framework for existing reactors and potential new reactors.

As the Advisory Committee on Reactor Safeguards recently stated in an April 24, 2006 letter on the review of ongoing security-related activities,

> "A variety of potential mitigation strategies have been identified for existing plants. The degree to which the risk due to security events can be reduced for existing plants is severely constrained by the cost of modifications in an existing plant. However, if incorporated into the design before construction and licensing, the cost of reducing the risk due to security events can be substantially reduced. The pilot studies performed for existing plants should be extended to examine the potential for increasing the robustness of new plants for security events and for including security considerations in the design certification process. Criteria for enhanced plant protection against security events at new reactors should be developed on a priority basis."

With regard to the current rulemaking, there are three important issues that I believe the staff should solicit comment on.

First, the staff should solicit comment on the need to establish a regulatory requirement to maintain communication protocols with the Nuclear Regulatory Commission in order to verify the authenticity of communications in a security event. The current rule establishes new reporting requirements for security-based events. The staff should solicit comments on whether these new requirements should include requirements for uniform protocols to verify the authenticity of reports under this new provision.

Second, the staff should expand on and solicit comment on the appropriate framework for the insider mitigation program requirements. I support amending the proposed rule prior to publication with the proposed language and structure presented to Commissioner McGaffigan and other Commissioner assistants on June 27, 2006.

Third, the staff should solicit comment on the need to establish performance-based security requirements for the transmission of vital plant information using the Emergency Response Data System (ERDS). ERDS is a crucial element of the NRC's incident response system in traditional accidents. Ensuring this important source of information can be transmitted during a security incident or even during a natural disaster will improve the NRC's ability to provide effective oversight of any emergency situation. Specifically, the staff should seek comment on using new technology that will both improve the performance of ERDS and improve the security of the system.

Lastly the staff should strive, to the extent possible, to make as much of the implementing guidance for all of these requirements publically available in order that all stakeholders can understand the requirements to which we hold our licensees in security. Making these requirements and the implementing guidance available to our stakeholders will go a long way toward instilling confidence that the NRC has required a much greater degree of security in a post-September 11, 2001 environment and will allow greater participation by stakeholders in the licensing process.

9/27/06

Gregory B. Jaczko Date

NOTATION VOTE

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: COMMISSIONER LYONS

SUBJECT: **SECY-06-0126 - PROPOSED RULEMAKING - POWER REACTOR SECURITY REQUIREMENTS (RIN 3150-AG63)**

Approved X w/comments & edits Disapproved _____ Abstain _____

Not Participating _____

COMMENTS:

Peter B. Lyons

SIGNATURE

6/ 28 /06

DATE

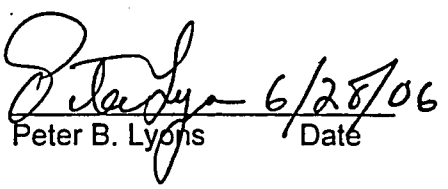
Entered on "STARS" Yes X No ___

## Commissioner Lyons' Comments on SECY-06-0126

I approve publishing in the *Federal Register* the proposed amendments to 10 CFR Parts 50, 72 and 73 with appendices. I approve certifying that this rule, if promulgated, will not have a negative economic impact on a substantial number of small entities in order to satisfy the requirements of the Regulatory Flexibility Act. The Order requirements addressed in the final rule should not be rescinded, but should be dispositioned as having been satisfied, if applicable, in individual cases.

I would like to highlight one matter that I wish to have clarified through this rulemaking regarding escorted access for members of the public visiting nuclear power reactors. In Europe, I have noticed that members of the public tour nuclear facilities and attend informational briefings at the facilities that enhance public education and awareness. I support these measures, and I would like to see more effort on the part of industry and the government to encourage the public to visit US nuclear power facilities and other US fuel cycle facilities. Therefore, this rulemaking should request public comment on the feasibility of a modified escorted access provision to selected areas of the facility for members of the public in order to facilitate this goal.

In addition, I have included edits to the rulemaking package, as attached hereto.



Peter B. Lyons Date 6/28/06

NRC Form 754) to the list of sections and forms with Office of Management of Management Budget (OMB) information collection requirements. A corrective revision to § 73.8 would also be made to reflect OMB approval of existing information collection requirements for NRC Form 366 under existing § 73.71.

- Section 73.70, "Records" would be revised to reference the appropriate revised paragraph numbers in proposed § 73.55 regarding the need to retain a record of the registry of visitors.

Additionally, § 73.81(b), "Criminal penalties" which sets forth the sections within Part 73 that are not subject to criminal sanctions under the AEA, would remain unchanged since willful violations of the newly proposed §§ 73.18, 73.19, and 73.58 may be subject to criminal sanctions.

Appendix B and Appendix C to Part 73 require special treatment in this rulemaking to preserve, with a minimum of conforming changes, the current requirements for licensees and applicants to whom this proposed rule would not apply. Accordingly, section I through V of Appendix B would remain unchanged, and the proposed new language for power reactors would be added as section VI. Appendix C would be divided into two sections, with Section I maintaining all current requirements, and Section II containing all proposed requirements related to power reactors.

## II. Rulemaking Initiation

On July 19, 2004, NRC staff issued a memorandum entitled "Status of Security-Related Rulemaking" (accession number ML041180532) to inform the Commission of plans to close former security-related actions and replace them with a comprehensive rulemaking plan to modify physical protection requirements for power reactors. This memorandum described rulemaking efforts that were suspended by the terrorist activities of September 11, 2001, and

2. Safety/Security interface requirements. These requirements are located in proposed § 73.58. The safety/security requirements are intended to explicitly require licensee coordination of potential adverse interactions between security activities and other plant activities that could compromise either plant security or plant safety. The proposed requirements would direct licensees to assess and manage these interactions so that neither safety nor security is compromised. These proposed requirements address, in part, a Petition for Rulemaking (PRM 50-80) that requested the establishment of regulations governing proposed changes to the facilities which could adversely affect the protection against radiological sabotage.

3. EPAct 2005 additional requirements. The EPAct 2005 requirements that would be implemented by this proposed rulemaking, in addition to the weapons-related additions described above, consist of new requirements to perform force-on-force exercises, and to mitigate potential conflicts of interest that could influence the results of NRC-observed force-on-force exercises. These proposed new requirements would be included in proposed § 73.55 and Appendix C to Part 73.

4. Accelerated notification and revised four-hour reporting requirements. This proposed rule contains accelerated security notification requirements (i.e., within 15 minutes) in proposed § 73.71 and Appendix G to Part 73 for attacks and imminent threats to power reactors. The proposed accelerated notification requirements are similar to what was provided to the industry in NRC Bulletin 2005-02, "Emergency Preparedness and Response Actions for Security-Based Events," dated July 18, 2005. The proposed rule also contains two new four-

18 years for unarmed responders, qualification scores for testing required by the training and qualification plan, qualification requirements for security trainers, qualification requirements of personnel assessing psychological qualifications, armorer certification requirements, and program requirements for on-the-job training.

10. Security Program Implementation insights. The proposed rule would impose new enhancements identified from implementation of the security orders, review of site security plans, and implementation of the enhanced baseline inspection program and force-on-force exercises. These new requirements would include changes to specifically require that the central alarm station (CAS) and secondary alarm station (SAS) have functionally equivalent capabilities such that no single act can disable the function of both CAS and SAS. The proposed additions would also include requirements for new reactor licensees to position the SAS within the protected area, add bullet resistance and limit the visibility into SAS. Proposed additions also require uninterruptible backup power supplies for detection and assessment equipment, "video-capture" capability, and qualification requirements for drill and exercise controllers.

11. Miscellaneous. The proposed rule would eliminate some requirements that the staff found to be unnecessary to ensure high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety, such as the requirement for guards to escort operators of motor vehicles within the protected area if the operators are cleared for unescorted access. The proposed

equivalent capabilities for both CAS and SAS. The security plans approved by the Commission on October 29, 2004, varied, due to the performance-based nature of the requirements, with respect to how the individual licensees implemented these requirements, but all sites were required to provide a CAS and SAS with functionally equivalent capabilities to support the implementation of the site protective strategy.

The proposed rule extends the requirement for no single act to remove capabilities to the key functions required of the alarm stations and would require licensees to implement protective measures such that a single act would not disable the intrusion detection, assessment, and communications capabilities of both the CAS and SAS. This proposed requirement would ensure continuity of response operations during a security event by ensuring that the detection, assessment, and communications functions required to effectively implement the licensee's protective strategy are maintained despite the loss of one or the other alarm station. For the purposes of assessing the regulatory burden of this proposed rule, the NRC assumed that all licensees would require assessments and approximately one third of the licensees would choose to implement hardware modifications.

The NRC has concluded that protecting the alarm stations such that a single act does not disable the key functions would provide an enhanced level of assurance that a licensee can maintain detection, assessment and communications capabilities required to protect the facility against the design basis threat of radiological sabotage. For new reactor licensees, licensed after the publication of this rule, the Commission would require CAS and SAS to be designed, constructed, and equipped with equivalent standards.

Uninterruptible Power for Intrusion Detection and Assessment Systems

Current regulatory requirements require back-up power for alarm annunciation and non-portable communication equipment, but do not require this back-up power to be uninterruptible. Although not specifically required, many licensees have installed uninterruptible power to their

response capabilities. Historically digital computer systems have played a limited role in the operation of nuclear power plants. However, the role of computer systems at nuclear power plants is increasing, as licensees take advantage of computer technology to maximize plant productivity. In general, licensees currently exclude from their access authorization programs, individuals who may electronically access equipment in the protected areas of nuclear power plants to perform their job functions, if their duties and responsibilities do not require physical unescorted access to the equipment located within protected or vital areas. However, because these individuals manage and maintain the networks that connect to equipment located within protected or vital areas and are responsible for permitting authorized and/or trusted personnel to gain electronic access to equipment and systems, they are often granted greater electronic privileges than the trusted and authorized personnel. With advancements in electronic technology and telecommunications, differences in the potential adverse impacts of a saboteur's actions through physical access and electronic access are lessening. Thus, the proposed rule would require those individuals who have authority to electronically access equipment that, if compromised, can adversely impact operational safety, security or emergency preparedness of the nuclear power plants, to be determined to be trustworthy and reliable.

The proposed revisions to § 73.56 would also address changes in the nuclear industry's structure and business practices since this rule was originally promulgated. At the time the current § 73.56 was developed, personnel transfers between licensees (i.e., leaving the employment of one licensee to work for another licensee) with interruptions in unescorted access authorization were less common. Most licensees operated plants at a single site and maintained an access authorization program that applied only to that site. When an individual left employment at one site and began working for another licensee, the individual was subject to a different access authorization program that often had different requirements. Because some licensees were reluctant to share information about previous employees with the new

would be specified in proposed § 73.56(m) [Protection of information]. As a result, individuals who are subject to this section would establish a detailed "track record" within the industry that would potentially cover their activities over long periods of time and would follow them if they change jobs and move to a new position that requires them to be granted unescorted access authorization by another licensee. The proposed requirement acknowledges the industry initiative to develop and utilize a database to ensure accurate information sharing between sites. This increased information sharing is necessary to provide high assurance that individuals who are granted and maintain unescorted access authorization are trustworthy and reliable when individuals move between access authorization programs. In addition, the increased information sharing would reduce regulatory burden on licensees when processing individuals who have had only short breaks between periods of unescorted access authorization.

Another change in the NRC's proposed approach to access authorization requirements is the result of a series of public meetings that were held with stakeholders during 2001–2004 to discuss potential revisions to 10 CFR Part, 26, "Fitness-for-Duty Programs." Part 26 establishes additional steps that the licensees who are subject to § 73.56 must take as part of the process of determining whether to grant unescorted access authorization to an individual or permit an individual to maintain unescorted access authorization. These additional requirements focus on aspects of an individual's behavior, character, and reputation related to substance abuse, and, among other steps, require the licensee and other entities who are subject to Part 26 to conduct drug and alcohol testing of individuals and an inquiry into the individual's past behavior with respect to illegal drug use or consumption of alcohol to excess, as part of determining whether the individual may be granted unescorted access authorization. However, historically there have been some inconsistencies and redundancies between the § 73.56 access authorization requirements and the related requirements in Part 26. These

notifications, the NRC may request the licensee establish a continuous communications channel after the licensee has made any emergency notifications to State officials or local law enforcement and if the licensee has taken action to stabilize the plant following any transient [associated with the 15-minute notification]. In NRC Bulletin 2005-02, "Emergency Preparedness and Response Actions for Security-Based Events," dated July 18, 2005, the NRC had indicated a continuous communications channel was not necessary for the new 15-minute notifications. However, in developing this proposed rule the Commission has evaluated the need to promptly obtain information of an unfolding event versus imposing an unreasonable burden on licensees in the midst of a rapidly unfolding event and possible plant transient. The Commission considers that the proposed regulation would provide a reasonable balance between these two objectives. Table 5 sets forth the proposed amendments to § 73.71 language as compared to the current language, and provides the supporting discussion for the proposed language. Table 8 sets forth the proposed amendments to the Appendix G language as compared to the current language, and provides the supporting discussion for the proposed language.

The Commission is interested in obtaining specific stakeholder input on the proposed changes to § 73.71 and Appendix G. Accordingly, the Commission is requesting persons commenting on this proposed rule to address the following question:

1. For the types of events covered by the proposed four-hour notification requirements in § 73.71 and Appendix G, should the notification time interval of all or some of these notifications be different (e.g., a 1-hour, 2-hour, 8-hour, 24-hour notification)? If so, what notification time interval is appropriate? State what is meant by notification time interval

IV.6. Appendix B to Part 73, "General Criteria For Security Personnel."

Table 11 (See Section VIII) is a cross-reference showing where individual requirements of the current regulation would be in the proposed regulation.

IV.8. Appendix G to Part 73, "Reportable Safeguards Events."

Proposed Appendix G to Part 73 provides requirements regarding the reporting of safeguards events. Proposed Appendix G would contain changes to support the revised and accelerated reporting requirements which would be incorporated into this rulemaking. Similar Proposed Appendix G would also contain revised four-hour reporting requirements that would require licensees to report to the NRC information of suspicious surveillance activities, attempts at access, or other information. Following September 11, 2001, the NRC issued guidance requesting that licensees report suspicious activities near their facilities to allow assessment by the NRC and other appropriate agencies. The proposed new reporting requirement will clarify this expectation to assure consistent reporting of this important information. Additionally, the proposed rule contains an additional four-hour reporting requirement for tampering events that do not meet the threshold for reporting under the current one-hour requirements. The proposed reporting requirements for tampering events will allow NRC assessment of these events. Table 8 sets forth the proposed amendments to Appendix G and provides the supporting discussion for the proposed language.

IV.9 Conforming and Corrective Changes.

The following conforming changes would also be made: §§ 50.34 and 50.54 (references to the correct paragraphs of revised Appendix C of Part 73), § 50.72 (changes to § 73.71 reports), §§ 72.212 and 73.70 (references to the correct paragraphs due to renumbering of § 73.55), and § 73.8 (adding § 73.18, § 73.19, and revised to reflect new NRC form 754 to

Table 1 - Proposed Sections 73.18 and 73.19

Firearms background check for armed security personnel and authorization for use of enhanced weapons.

| PROPOSED LANGUAGE | CONSIDERATIONS |
|---|---|
| § 73.18 Firearms background check for armed security personnel. | This new section would implement the firearms background check requirements of the new § 161A.b. of the Atomic Energy Act of 1954, |
| (a) *Introduction.* (1) Licensees and certificate holders listed under paragraph (b) of this section shall ensure that a firearms background check is completed in accordance with this section for all security personnel assigned duties requiring access to a covered weapon at the licensee's or certificate holder's facility. | This section would require a firearms background check for all security personnel with access to covered weapons (i.e., armed duties) [see also new definition of *covered weapon* in § 73.2 at the end of this Table]. These background checks would only be required for security personnel who are protecting certain Commission-regulated facilities [specified in paragraph (b)].<br>The Commission considers duties "requiring access to any covered weapon" would include such duties as: security operations and training and weapons' maintenance, handling, accountability, transport, and use. |

| | |
|---|---|
| § 73.18(c)(2) *NRC Form 754.* (i) Licensees and certificate holders shall submit to the NRC, in accordance with § 73.4, an NRC Form 754 for all security personnel requiring a firearms background check under this section.<br>(ii) Licensees and certificate holders shall retain a copy of all NRC Forms 754 submitted to the NRC for a period of one (1) year subsequent to the termination of an individual's access to covered weapons or to the denial of an individual's access to covered weapons. | This paragraph would require licensees and certificate holders to submit to the Commission a completed NRC Form 754 for each individual assigned armed duties. Licensees and certificate holders would submit these forms via paper or electronic means under the applicable regulation (see § 73.4) Licensees and certificate holders would be required to retain submitted forms as a record for a period of 1 year after the individual's security officer's access to covered weapons is terminated or denied.<br>NRC Form 754 would require individuals to provide certain identifying information to the Commission. A proposed draft NRC Form 754 is located in the NRC's ADAMS system as described in Section VIII of this notice, and comments on this form and its estimated burden may be submitted to the Commission as set forth under ADDRESSES. |

| | |
|---|---|
| § 73.18(c)(9) *Violations of law.* The NRC will report instances of prohibited persons possessing or receiving covered weapons in violation of Federal law to the appropriate Federal agency, or in violation of State law to the appropriate State agency. | The NRC is obligated to report (potential or possible) violations of Federal or State law it becomes aware of to the appropriate agency (e.g., persons prohibited from possessing or receiving covered weapons who are actually performing armed security duties). |

| | |
|---|---|
| § 73.19(d) *Approval process.*<br>(1) *Commission approval.* (i) Licensees and certificate holders specified in paragraph (b) of this section who choose to utilize enhanced weapons as part of their physical protection program, shall submit to the Commission for prior review and written approval, new or revised physical security plans, training and qualification plans, safeguards contingency plans, and a safety assessment incorporating the use of the specific enhanced weapons the licensee or certificate holder intends to use. Licensees or certificate holders shall submit such revised plans for prior Commission review and written approval notwithstanding the provisions of §§ 50.54(p), 70.32(e), and 76.60 of this chapter. | This paragraph would describe the process for Commission approval of a licensees or certificate holders plans to use enhanced weapons. The use of such weapons would be incorporated into security plans for prior Commission review and approval. This paragraph would also require the submission of a new safety assessment evaluation of the onsite and offsite impacts from the use of the enhanced weapons (in protecting the facility or from training activities). Submission of such revised plans for prior review and approval would be required irrespective of whether the licensees or certificate holder concludes the use of these enhanced weapons would not cause "a decrease in security effectiveness." |

| | |
|---|---|
| § 73.2 Definitions. | Would add three new definitions to this section as conforming changes to the new §§ 73.18 and 73.19 for *covered weapon*, *enhanced weapon*, and *standard weapon*. Other new definitions that would be added as conforming changes to this section in support of other regulations (e.g., *safety/security interface* and *target set*) are discussed in other Tables under this notice. |

| | | |
|---|---|---|
| | (a)(6)(ii) Licensees shall comply with the requirements of paragraph (i)(4) such that both alarm stations are provided with equivalent capabilities for detection, assessment, monitoring, observation, surveillance, and communications. | This requirement would be added for consistency with and clarification of the proposed requirement of (i)(4) and to clarify that for new reactors, both the central and secondary alarm stations must be provided "equivalent capabilities" and not simply equivalent "functional" capabilities as is stated in the proposed (i)(4). The Commission has determined that these capabilities must be equivalent for new reactors to ensure that the secondary alarm station is truely redundant to the central alarm station. |

| | | |
|---|---|---|
| 10 CFR 73.55(c)(2) The physical barriers at the perimeter of the protected area shall be separated from any other barrier designated as a physical barrier for a vital area within the protected area. | (e)(6)(ii) The protected area perimeter physical barriers must be separated from any other barrier designated as a vital area physical barrier, unless otherwise identified in the approved physical security plan. | This requirement would be retained with minor revision. The phrase "unless otherwise identified in the approved physical security plan" would be added to provide flexibility for an alternate methodology to be described in the Commission approved security plans. |
| 73.55(e)(3) All emergency exits in each protected area and each vital area shall be alarmed. | (e)(6)(iii) All emergency exits in the protected area must be secured by locking devices that allow exit only, and alarmed. | This requirement would retain and separate the two current requirements with minor revision. The phrase "secured by locking devices which allow exit only" would be added to provide a performance based requirement relative to the function of locking devices with emergency exit design to prevent entry. Vital areas would be addressed in the proposed § 73.55(e)(8)(vii). |

| | | |
|---|---|---|
| § 73.55(c)(1) The licensee shall locate vital equipment only within a vital area, which in turn, shall be located within a protected area such that access to vital equipment requires passage through at least two physical barriers of sufficient strength to meet the performance requirements of Paragraph (a) of this section. | (e)(7)(i) Vital equipment must be located only within vital areas, which in turn must be located within protected areas so that access to vital equipment requires passage through at least two physical barriers designed and constructed to perform the required function, except as otherwise approved by the Commission in accordance with paragraph (f)(2) below. | This requirement would be retained with minor revision. The phrase "of sufficient strength to meet the performance requirements of Paragraph (a) of this section" would be replaced with the phrase "that meet the requirements of this section" for consistency with the proposed requirements for physical barriers discussed throughout this proposed § 73.55(e). The phrase "except as otherwise ~~identified in accordance with § 73.55(f)(2) below~~" would be added to account for the condition addressed by that paragraph. |
| § 73.55(c)(1) More than one vital area may be located within a single protected area. | (e)(7)(ii) More than one vital area may be located within a single protected area. | This requirement would be retained. |

| | | |
|---|---|---|
| § 73.55(e)(1) The onsite central alarm station must be considered a vital area and...<br>§ 73.55(e)(1) Onsite secondary power supply systems for alarm annunciator equipment and non-portable communications equipment as required in Paragraph (f) of this section must be located within vital areas. | (e)(7)(iii) The reactor control room, the spent fuel pool, secondary power supply systems for intrusion detection and assessment equipment, non-portable communications equipment, and the central alarm station, must be provided protection equivalent to vital equipment and located within a vital area. | This requirement would retain and combine two current requirements from 10 CFR 73.55(e)(1), for protecting these areas equivalent to a vital area. The Commission added the "spent fuel pool" to emphasize the Commission view that because of changes to the threat environment the spent fuel pool must also be provided this protection. The phrase "alarm annunciator" would be replaced with "intrusion detection and assessment" to clarify the application of this proposed requirement to intrusion detection sensors and video assessment equipment as well as the alarm annunciation equipment. |

| | | |
|---|---|---|
| | (e)(9)(i) The licensee shall control waterway approach routes or proximity to any area from which a waterborne vehicle, its personnel, or its contents could disable the personnel, equipment, or systems necessary to meet the performance objective and requirements described in paragraph (b). | This requirement would be added to provide a requirement for controlling waterway approach routes consistent with the requirement of the proposed (e)(9)(ii). Because of changes to the threat environment, the Commission views waterway approach routes and control measures to be a critical element of the onsite physical protection program and one that requires continual analysis and evaluation to maintain effectiveness. |
| | (e)(9)(ii) The licensee shall delineate areas from which a waterborne vehicle must be restricted and install waterborne vehicle control measures, where applicable. | This requirement would be added to provide a requirement for notifying individually unauthorized personnel that access is not permitted and the installation of barriers where appropriate. |

| | | |
|---|---|---|
| | | Based on changes to the threat environment, the Commission has determined that the proposed requirement is necessary to facilitate licensee achievement of the performance objective of the proposed paragraph (b). |
| | (g)(2) In accordance with the approved security plans and before granting unescorted access through an access control point, the licensee shall: | This requirement would be added to specify the basic functions that must be satisfied to meet the current and proposed requirements for controlling access into any area for which access controls are implemented. |
| § 73.55(d)(1) Identification...of all individuals unless otherwise provided herein must be made and... | (g)(2)(i) Confirm the identity of individuals. | This requirement would retain the current requirement with minor revisions for formatting purposes. |

| | | |
|---|---|---|
| | (g)(2)(iv) Confirm, in accordance with industry shared lists and databases, that individuals are not denied access to another licensed facility. | This requirement would be added to describe an acceptable information sharing mechanism used by licensees to share information about visitors and employees who have requested either escorted or unescorted access to at least one site. Based on changes to the threat environment, the Commission has determined that this proposed requirement would be a prudent enhancement to the licensee capabilities. |
| | (g)(3) Access control points must be: | This header would be added for formatting purposes. |

| | | |
|---|---|---|
| | (g)(4)(iii) The licensee shall ensure that restrictions for site access and egress during emergency conditions are coordinated with responses by offsite emergency support agencies identified in the site emergency plans. | This requirement would be added to provide a performance based requirement for coordination of security access controls during emergencies with the access needs of emergency response personnel. This proposed requirement is intended to provide the necessary level of flexibility to the licensee to ensure access by appropriate personnel while maintaining the necessary security posture for controlling access to areas where dangerous conditions exit such as a violent conflict involving weapons. |
| | (g)(5) Vehicles. | This header would be added for formatting purposes. |

| | | |
|---|---|---|
| § 73.55(d)(8) All keys, locks, combinations, and related access control devices used to control access to protected areas and vital areas must be controlled to reduce the probability of compromise. | (g)(6)(ii) Keys, Locks, Combinations, and Passwords. All keys, locks, combinations, passwords, and related access control devices used to control access to protected areas, vital areas, security systems, and safeguards information must be controlled and accounted for to reduce the probability of compromise. The licensee shall: | This requirement would be retained and revised with minor revisions. Most significantly, the word "passwords" would be added to account for technological advancements associated with the use of computers. The phrase "security systems, and safeguards information" would be added to emphasize the need to control access to these items. The phrase "and accounted for " would be added to confirm possession by the individual's to whom the access control device has been issued. |

| | | |
|---|---|---|
| § 73.55(d)(8) Whenever there is evidence or suspicion that any key, lock, combination, or related access control devices may have been compromised, it must be changed or rotated. | (g)(6)(ii)(C) Implement compensatory measures upon discovery or suspicion that any access control device may have been compromised. Compensatory measures must remain in effect until the compromise is corrected. | This requirement would be retained and revised to provide a performance based requirement for compensatory measures taken in response to compromise. Most significantly, the phrase "it must be changed or rotated" would be captured in the proposed § 73.55(g)(6)(ii) (D) and (E). The phrase "key, lock, combination, or related" would be replaced with the phrase "in use or spare" to ensure focus on these items. The phrase "Compensatory Measures must remain in effect until the compromise is corrected" would be added to provide focus specific to when compensatory measures would no longer apply. |

| | | |
|---|---|---|
| | (g)(7)(i)(B) Confirm the identity of each visitor through physical presentation of an identification card issued by a recognized local, state, or Federal Government agency that includes a photo or contains physical characteristics of the individual requesting escorted access. | This requirement would be added to require the verification of the true identity of non-employee individuals through the presentation of photographic government issued identification (i.e., driver's license) which provides physical characteristics that can be compared to the holder. The word "recognized" would be used to provide flexibility for other types of identification that may be issued by local, state or federal governments. |

| | | |
|---|---|---|
| | (g)(8) Escorts. The licensee shall ensure that all escorts are trained in accordance with Appendix B to this part, the approved training and qualification plan, and licensee policies and procedures. | This requirement would be added to provided performance based requirements for satisfying the escort requirements of this proposed rule and would provide regulatory stability through the consistent application of visitor controls at all sites. Based on changes to the threat environment, the Commission has determined that emphasis on the identification and control of visitors is a prudent and necessary enhancement to facilitate licensee achievement of the performance basis of the proposed (b)(1). |

paragraph

| | | |
|---|---|---|
| | (h)(5) Vehicle search procedures must be performed by at least two (2) properly trained and equipped security personnel, at least one of whom is positioned to observe the search process and provide a timely response to unauthorized activities if necessary. | This requirement would be added to provide a performance based requirement for performing vehicle searches. This proposed requirement would ensure that unauthorized activities would be identified and a timely response would be initiated at a vehicle search area, to include an armed response. Based on changes to the threat environment, the Commission has determined that this requirement would facilitate achievement of the performance objective and requirements of the proposed paragraph (b). |
| § 73.55(d)(4) Vehicle areas to be searched shall include the cab, engine compartment, undercarriage, and cargo area. | (h)(6) Vehicle areas to be searched must include, but are not limited to, the cab, engine compartment, undercarriage, and cargo area. | This requirement would be retained with minor revisions. |

| | | |
|---|---|---|
| § 73.55(d)(1) ...except bona fide Federal, State, and local law enforcement personnel on official duty to these equipment searches upon entry into a protected area.<br>§ 73.55(d)(4) ...except under emergency conditions, shall be searched for items which could be used for sabotage purposes prior to entry into the protected area. | (h)(8) Exceptions to the search requirements of this section must be identified in the approved security plans. Submitted to the Commission for prior review and approval and must be | This requirement would retain, combine, and revise two current requirements § 73.55(d)(1) and (4) to generically account for those instances where search requirements would not be met before granting access beyond a physical barrier. This proposed requirement would require that the licensee specify in the approved plans the specific circumstances under which search requirements would not be satisfied. |

| | | |
|---|---|---|
| | (i)(3) The licensee's intrusion detection system must be designed to ensure that both alarm station operators:<br>(i)(3)(i) Are concurrently notified of the alarm annunciation.<br>(i)(3)(ii) Are capable of making a timely assessment of the cause of each alarm annunciation.<br>(i)(3)(iii) Possess the capability to initiate a timely response in accordance with the approved security plans, licensee protective strategy, and implementing procedures. | This requirement would be added to provide performance based requirements consistent with the current § 73.55(e)(1), and the proposed requirements of this proposed section. The proposed requirement for dual knowledge and dual capability within both alarm stations provides a defense-in-depth component consistent with the proposed requirement for protection against a single act. Based on changes to the threat environment the Commission has determined this proposed requirement is a prudent and |

| | | |
|---|---|---|
| | | necessary clarification of current requirements necessary to facilitate the licensee capability to achieve the performance objective of the proposed paragraph (b)(1). |

| | | |
|---|---|---|
| | (i)(7)(iv) Provide visual and audible alarm annunciation and concurrent video assessment capability to both alarm stations in a manner that ensures timely recognition, acknowledgment and response by each alarm station operator in accordance with written response procedures. | This requirement would be added for consistency with the proposed requirement for equivalent capabilities in both alarm stations. The phrase "visual and audible" would provide redundancy to ensure that each alarm would be recognized and acknowledged when received. |
| § 73.55(e)(2) ...e.g., an automatic indication is provided when failure of the alarm system or a component occurs, or when the system is on standby power. | (i)(7)(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. | This requirement would be retained with minor revision for formatting purposes. |

| | | |
|---|---|---|
| § 73.70(f) A record at each onsite alarm annunciation location of each alarm, false alarm, alarm check, and tamper indication that identifies the type of alarm, locations, alarm circuit, date, and time. In addition, details of response by facility guards and watchmen to each alarm, intrusion, or other incident shall be recorded. | (i)(7)(vi) Maintain a record of all alarm annunciations, the cause of each alarm, and the disposition of each alarm. | This requirement would be added for consistency with § 73.70(f). The Commission has determined that this record would be a commonly maintained record in electronic form as an automatic function of intrusion detection systems used by industry and would therefore be a prudent and necessary requirement. |
| | (i)(8) Alarm Stations. | This header would be added for formatting purposes. |
| § 73.55(e)(1) All alarms required pursuant to this part must annunciate in a continuously manned central alarm station located within the protected area and in at least one other continuously manned station... | (i)(8)(i) Both alarm stations must be continuously staffed by at least one trained and qualified member of the security organization. | This requirement would retain the current requirement § 73.55(e)(1) for continuously staffed alarm stations and would be revised to describe the necessary qualifications that would be required of the assigned individuals. |

| | | |
|---|---|---|
| | (i)(8)(iv) The licensee shall assess and respond to all alarms and other indications of unauthorized activities in accordance with the approved security plans and implementing procedures. | This requirement would be added to for consistency with current requirements. The specific requirements of the current § 73.55(h)(4) are retained in detail in the proposed Appendix C. |
| | (i)(8)(v) The licensee implementing procedures must ensure that both alarm station operators are knowledgeable of all alarm annunciations, assessments, and final disposition of all alarms, to include but not limited to a prohibition from changing the status of a detection point or deactivating a locking or access control device at a protected or vital area portal, without the knowledge and concurrence of the other alarm station operator. | This requirement would be added for consistency with related requirements of this proposed section and to ensure that the licensee provides a process by which both alarm station operators are concurrently made aware of each alarm and are knowledgeable of how each alarm is resolved and that no one alarm station operator can manipulate alarm station equipment, communications, or procedures without the knowledge and concurrence of the other. |

| | | |
|---|---|---|
| | (i)(9)(ii)(A) Continual surveillance, observation, and monitoring responsibilities must be performed by security personnel during routine patrols or by other trained and equipped personnel designated as a component of the protective strategy. | This requirement would be added to provide necessary qualifying requirements for performance of observation and monitoring activities. The word "continual" would mean the same as used in the proposed (i)(9)(ii). |
| | (i)(9)(ii)(B) Surveillance, observation, and monitoring requirements may be accomplished by direct observation or video technology. | This requirement would be added to provide a performance based requirement for ensuring surveillance, observation, and monitoring capabilities that may be met through the use of video technology or direct human observation. |

| | | |
|---|---|---|
| § 73.55(f)(1) ...who shall be capable of calling for assistance from other guards, watchmen, and armed response personnel and from local law enforcement authorities. | (j)(2) Individuals assigned to each alarm station shall be capable of calling for assistance in accordance with the approved security plans, licensee integrated response plan, and licensee procedures. | This requirement would be retained with minor revision. Most significantly, in order to provide flexibility and to capture the proposed requirements of Appendix C for an Integrated response Plan, this proposed requirement replaces the specific list of support entities to be called with a performance based requirement to follow predetermined actions. |
| § 73.55(f)(1) Each guard, watchman or armed response individual on duty shall be capable of maintaining continuous communication with an individual in each continuously manned alarm station required by paragraph (e)(1) of this section... | (j)(3) Each on-duty security officer, watchperson, vehicle escort, and armed response force member shall be capable of maintaining continuous communication with an individual in each alarm station. | This requirement would be retained with minor revisions. Most significantly, this proposed requirement update the titles used to identify the listed positions and would add "vehicle escorts" for consistency with the proposed paragraph (g)(8). |

| | | |
|---|---|---|
| | (l)(2) Commercial nuclear power reactors using MOX fuel assemblies are exempt from the requirements of §§ 73.20, 73.45, and 73.46 for the onsite physical protection of unirradiated MOX fuel assemblies. | This requirement would be added because the Commission has determined that due to the low plutonium concentration, composition of the MOX fuel, and configuration (size and weight) of the assemblies, the physical security protection measures identified in the listed regulations are superceded by those requirements addressed in this proposed section for unirradiated MOX fuel assemblies at nuclear power reactor facilities. |
| | (l)(3) Administrative Controls. | This header would be added for formatting purposes. |

| | | |
|---|---|---|
| | (l)(4)(v) Removal of locks used to secure equipment and power sources required for the movement of unirradiated MOX fuel assemblies or openings to areas containing unirradiated MOX fuel assemblies must require approval by both the on-duty security shift supervisor and the operations shift manager. | This requirement would be added to ensure that the licensee both security and operations management level personnel would be responsible for the removal of locks securing MOX fuel assemblies. |
| | (l)(4)(v)(A) At least one armed security officer shall be present to observe activities involving the movement of unirradiated MOX fuel assemblies before the removal of the locks and providing power to equipment required for the movement or handling of unirradiated MOX fuel assemblies. | This requirement would be added to ensure that immediate armed response capability is provided before accessing equipment used to move unirradiated MOX fuel assemblies. |

| | | |
|---|---|---|
| | (l)(4)(v)(B) At least one armed security officer shall be present at all times until power is removed from equipment and locks are secured. | This requirement would be added to ensure that immediate armed response capability is provided during any activity involving the use of equipment used required to move unirradiated MOX fuel assemblies. |
| | (l)(4)(v)(C) Security officers shall be trained and knowledgeable of authorized and unauthorized activities involving unirradiated MOX fuel assemblies. | This requirement would be added to ensure that assigned security officers possess the capability to immediately recognize, report, and respond to unauthorized activities involving unirradiated MOX fuel assemblies. |

| | | |
|---|---|---|
| | (m)(1) The licensee shall implement a cyber-security program that provides high assurance that computer systems, which if compromised, would adversely impact safety, security, and emergency preparedness, are protected from cyber attacks. | This requirement would be to ensure that nuclear power plants are protected from cyber attacks via minimizing the potential attack pathway and the consequences arising from a successful cyber attack. |

| | | |
|---|---|---|
| | (m)(1)(i) The licensee shall describe the cyber-security program requirements in the approved security plans. | This requirement would added to ensure licensees to have a comprehensive security plan by integrating cyber-security into the overall onsite physical protection program. As licensees take advantage of computer technology to maximize plant productivity, the role of computer systems at nuclear power plants is increasing, the Commission has determined that incorporation of a cyber-security program into the Commission approved security plans would be a prudent and necessary security enhancement. |

| | | |
|---|---|---|
| | (m)(4)(i) The licensee shall implement a cyber-security incident response and recovery plan to minimize the adverse impact of a cyber-security incident on safety, security, or emergency preparedness systems. | This requirement would be added to ensure that each licensee would be prepared to respond to computer security incidents in a manner that ensures that plants are safe and secure. A computer security incident could result from a computer virus, other malicious code, or a system intruder, either an insider or as a result of an external attack and could adversely impact the licensees ability to effectively maintain safety, security, or emergency preparedness. Without an incident response and recovery plan, |

| | | |
|---|---|---|
| | | licensees would respond to a computer security incident in an ad hoc manner. However with an incident response and recovery plan, licensees would respond to an incident in a quick and organized manner. This would minimize the adverse impact caused by a computer security incident. |

| | | |
|---|---|---|
| § 73.55(d)(7)(ii)(B) Periodically review physical security plans and contingency plans and procedures to evaluate their potential impact on plant and personnel safety. | (n)(3) The licensee shall periodically review the approved security plans, the integrated response plan, the licensee protective strategy, and licensee implementing procedures to evaluate their effectiveness and potential impact on plant and personnel safety. | This requirement would be retained with minor revision. The phrase "Integrated Response Plan" would be added to emphasize the importance of this proposed plan and to emphasize its relationship to other site plans. The term "implementing" procedures would be added for consistency with this proposed section. |
| | (n)(4) The licensee shall periodically evaluate the cyber-security program for effectiveness and shall update the cyber-security program as needed to ensure protection against changes to internal and external threats. | This requirement would be added to account for the use of computers and the need to ensure that required protective measures are being met and to evaluate the effects that changes or other technological advancements would have on systems used at nuclear power plants. |

| | | |
|---|---|---|
| § 73.55(g)(2) Each intrusion alarm shall be tested for performance at the beginning and end of any period that it is used for security. | (o)(3) Intrusion detection and access control equipment must be performance tested in accordance with the approved security plans. | This requirement would be retained and revised to correct the periodicity of performance testing stated in the current § 73.55(g)(2) and to add "access control equipment" due to the widespread use of access control technologies and to focus on the need to ensure that this equipment is functioning as intended in response to the predetermined stimuli (i.e., biometrics). The phrase "each intrusion alarm" would be replaced with the phrase "Intrusion detection and access control equipment" to more accurately describe the equipment to be performance tested. |

| | | |
|---|---|---|
| § 73.55(c)(8)(ii) The Commission will approve the proposed alternative measures if they provide substantial protection against a land vehicle bomb, and it is determined by an analysis, using the essential elements of 10 CFR 50.109, that the costs of fully meeting the design goals and criteria are not justified by the added protection that would be provided. | (t)(4) Alternative Vehicle Barrier Systems. In the case of alternative vehicle barrier systems required by § 73.55(e)(8), the licensee shall demonstrate that:<br>(t)(4)(i) the alternative measure provides substantial protection against a vehicle bomb, and<br>(t)(4)(ii) based on comparison of the costs of the alternative measures to the costs of meeting the Commission's requirements using the essential elements of 10 CFR 50.109, the costs of fully meeting the Commission's requirements are not justified by the protection that would be provided. | This requirement would be retained with minor revision. The phrase "The Commission will approve the proposed alternative measures" would be deleted because it would be unnecessary. The proposed language clearly stipulates that alternative measures will be reviewed by the staff and approval would be contingent upon the justification provided by the licensee to include an analysis. |

| | | |
|---|---|---|
| | (a)(4) The licensee is responsible to the Commission for maintaining the authorization program in accordance with Commission regulations and related Commission-directed orders through the implementation of the approved program and site implementing procedures. | This requirement would added to clarify that the licensee is responsible for meeting Commission regulations and the approved security plans. The phrase "through the implementation of the approved program and site implementing procedures" would be added to describe the relationship between Commission regulations, the approved authorization program, and implementing procedures. The Commission views the approved security plans as the mechanism through which the licensee meets Commission requirements through implementation, therefore, the licensee is responsible to the Commission for this performance. |

| | | |
|---|---|---|
| pursuant to §§ 50.21(b) or 50.22 of this chapter and each applicant for a combined construction permit and operating license pursuant to part 52 of this chapter, whose application is submitted after April 25, 1991, shall include the required access authorization program as part of its Physical Security Plan. The applicant, upon receipt of an operating license or upon receipt of operating authorization, shall implement the required access authorization program as part of its site | | approved access authorization program when approval to begin operating is received. This proposed requirement would also add a requirement for Commission review and approval of an applicants Physical Security Plan incorporating the requirements of this proposed section for the reasons discussed with respect to proposed § 73.56(a)(1). The Commission intends to delete the current § 73.56(a)(2) because there are no remaining applicants for an operating license under §§ 50.21(b) or 50.22 of this |

| | | |
|---|---|---|
| | | background investigation; psychological assessment; behavioral observation; a review procedure for adverse determinations regarding an individuals' trustworthiness and reliability; audits; the protection of information; and retaining and sharing records. The phrase, "to the extent that the licensees and applicants rely upon C/V authorization programs or program elements," would be used in proposed § 73.56(a)(6) to clarify that C/Vs need only meet the requirements of this section for those authorization program elements upon |

| | | |
|---|---|---|
| | | engineers or information technology technicians to take actions from remote locations that may affect the operability of safety-related components, or affect the functionality of operating systems. Because the potential impact of actions taken through electronic means may be as serious as actions taken by an individual who is physically present within a protected or vital area, the NRC has determined that subjecting this additional category of individuals to the AA program is necessary to ensure public health and safety and the common defense and security. |

| | | |
|---|---|---|
| | | strategy, which may include individuals who are not armed. In practice, the NRC is not aware of any licensees, applicants, or C/Vs who do not subject this broader category of individuals to an AA program. However, the proposed rule would specify that these individuals shall be subject to an AA program because of their critical responsibilities with respect to assuring plant security and, therefore, the need for high assurance that they are trustworthy and reliable. |

| | | |
|---|---|---|
| (b) *General performance objective and requirements.* (1) The licensee shall establish and maintain an access authorization program granting individuals unescorted access to protected and vital areas with the objective of providing high assurance that individuals granted unescorted access are trustworthy and reliable, and do not constitute an unreasonable risk to the health and safety of the public including a potential to commit radiological sabotage. | (c) General performance objective. Access authorization programs must provide high assurance that the individuals who are specified in paragraph (b)(1), and, if applicable, (b)(2) of this section are trustworthy and reliable, and do not constitute an unreasonable risk to public health and safety or the common defense and security, including the potential to commit radiological sabotage. | Proposed § 73.56(c) would retain the meaning of the current program performance objective, which is embedded in current § 73.56(b), but would separate it from the requirement in the current paragraph for licensees to establish and maintain an AA program. The requirement to establish and maintain AA programs would be moved to proposed § 73.56(a), where it would be imposed on each entity who would be subject to the section, for organizational clarity. The performance objective would be revised to add cross-references to the categories of individuals who must be subject to an authorization |

| | | |
|---|---|---|
| | (d)(1) Informed consent. The licensees, applicants, and C/Vs specified in paragraph (a) of this section may not initiate any element of a background investigation without the knowledge and written consent of the subject individual. licensees, applicants, and C/Vs shall inform the individual of his or her right to review information collected to assure its accuracy, and provide the individual with an opportunity to correct any inaccurate or incomplete information that is developed by licensees, applicants, and C/Vs about the individual. | Proposed §73.56(d)(1) would require the entities who are subject to this section to obtain written consent from any individual who is applying for UAA before the licensee, applicant, or C/V initiates any element of the background investigation that is required in this section. The practice of obtaining the individual's written consent for the background investigation has been endorsed by the NRC and incorporated into licensees' Physical Security Plans since § 73.56 was first promulgated. It is necessary to protect the privacy rights of individuals who are applying for UAA. The proposed paragraph would also require licensees, |

| | | |
|---|---|---|
| | | In the past, licensees' AA program procedures limited the number of years of the individual's credit history that reviewing officials were required to consider in determining an individual's trustworthiness and reliability. As a result, some reviewing officials may not have considered credit history information for several years, even if the reporting agency provided it. As a result, individuals who were subject to different authorization programs were evaluated inconsistently. Furthermore, credit history reporting agencies also provide employment data that can be compared to the information disclosed by |

| | | |
|---|---|---|
| | (f)(2) Behavioral observation must be conducted by the individuals specified in paragraph (b)(1) and, if applicable, (b)(2). The licensees, applicants, and C/Vs specified in paragraph (a) of this section shall ensure that individuals who are subject to this section successfully complete behavioral observation training. | The proposed paragraph would amend the portion of current § 73.56(b)(2)(iii) that requires only supervisors and management personnel to conduct behavioral observation by requiring all individuals who are subject to an authorization program to conduct behavioral observation. Increasing the number of individuals who conduct behavioral observation would enhance the effectiveness of AA programs by increasing the likelihood of detecting behavior or activities that may be adverse to the safe operation and security of the facility and may, therefore, constitute an unreasonable risk to the health and safety |

| | | |
|---|---|---|
| | (f)(3) Individuals who are subject to an authorization program under this section shall report to the reviewing official any concerns arising from behavioral observation, including, but not limited to, concerns related to any questionable behavior patterns or activities of others. Licensees, applicants and CVs shall not tolerate false reporting and other abuses of this requirement. | Proposed § 73.56(f)(3) would require individuals to report any concerns arising from behavioral observation to the licensee's, applicant's, or C/V's reviewing official. This specificity is necessary because the NRC is aware of past instances in which individuals reported concerns to supervisors or other licensee personnel who did not then inform the reviewing official of the concern. As a result, the concern was not addressed and any implications of the concern for the individual's trustworthiness and reliability were not evaluated. Therefore, the proposed rule would require individuals to |

| | | |
|---|---|---|
| (c) *Existing, reinstated, transferred, and temporary access authorization.* (1) Individuals who have had an uninterrupted unescorted access authorization for at least 180 days on April 25, 1991 need not be further evaluated. Such individuals shall be subject to the behavioral observation requirements of this section. | (c)(1) Deleted. | The proposed rule would eliminate current § 73.56(c)(1), which permitted individuals who had an uninterrupted unescorted access authorization for at least 180 days on April 25, 1991, to retain unescorted access authorization and required them to be subject to behavioral observation. The current paragraph would be eliminated because these requirements no longer apply. |
| (c) *Existing, reinstated, transferred, and temporary access authorization.* | (h) Granting unescorted access authorization. The licensees, applicants, and C/Vs specified in paragraph (a) of this section shall implement the | Proposed § 73.56(h) would replace and amend current § 73.56(c), which permits AA programs to specify conditions for reinstating an interrupted UAA, for |

| | | |
|---|---|---|
| | if, upon review and evaluation, the reviewing official determines that such access is warranted.<br>Licensees and applicants shall develop re-instatement review procedures for assessing individuals who have been in an access-denied status | areas as visitors. Licensees' current Physical Security Plans require that any visitor to a protected area or vital area must be escorted and under the supervision of an individual who has UAA and, therefore, is trained in behavioral observation, in accordance with the requirements of this section and related requirements in Part 26. However, in the current threat environment, the NRC believes that permitting any individual who has been determined not to be trustworthy and reliable to enter protected or vital areas does not adequately protect public health and safety or the common defense and security. Therefore, |

| | | |
|---|---|---|
| | (k)(2) Authorization program personnel. Licensees, applicants and C/Vs shall ensure that any individual who evaluates personal information for the purpose of processing applications for unescorted access authorization including, but not limited to a clinical psychologist of psychiatrist who conducts psychological assessments under paragraph (e) of this section; has unfettered access to the files, records, and personal information associated with individuals who have applied for unescorted access authorization; or is responsible for managing any databases that contain | A new § 73.56(k)(2) would require that individuals who evaluate and have access to any personal information that is collected for the purposes of this section must be determined to be trustworthy and reliable, and establishes two alternative methods for making this determination. Proposed § 73.56(k)(2)(i) would permit licensees, applicants, and C/Vs to subject such individuals to the process established in this proposed section for granting UAA. Proposed § 73.56(k)(2)(ii) would permit licensees, applicants, or C/Vs to subject such individuals to the requirements for granting UAA in proposed paragraphs |

| | | |
|---|---|---|
| | | requirements would be added for the reasons discussed with respect to proposed § 73.56(k). |
| (e) *Review procedures.* Each licensee implementing an unescorted access authorization program under the provisions of this section shall include a procedure for the review, at the request of the affected employee, of a denial or revocation by the licensee of unescorted access authorization of an employee of the licensee, contractor, or vendor, which adversely affects employment. The procedure must provide that the employee is informed of the grounds for denial or revocation and allow the employee an opportunity to provide additional relevant information, and | (l) Review procedures. Each licensee, applicant, and C/V who is implementing an authorization program under this section shall include a procedure for the review, at the request of the affected individual, of a denial or unfavorable termination of unescorted access authorization which adversely affects employment. The procedure must require that the individual is informed of the grounds for the denial or unfavorable termination and allow the individual an opportunity to provide additional relevant information, and provide an opportunity for an objective review of the information | Proposed § 73.56(l) would retain the meaning of current § 73.56(e) but update some of the terms used in the provision. The proposed paragraph would replace the term, "revocation," with the term, "unfavorable termination," for the reasons discussed with respect to proposed paragraph (d)(1)(iii) of this section. In addition, the proposed paragraph would add references to applicants to reflect the NRC's new licensing processes for nuclear power plants, as discussed with respect to proposed § 73.56(a). Reference to C/Vs would also be added for completeness, as discussed with respected to proposed |

| | | |
|---|---|---|
| (i) Other licensees, contractors, or vendors, or their authorized representatives, legitimately seeking the information as required by this section for unescorted access decisions and who have obtained a signed release from the individual. | (m)(2) Personal information that is collected under this section must be disclosed to other licensees, applicants, and C/Vs, or their authorized representatives, who are legitimately seeking the information for unescorted access authorization determinations under this section and who have obtained a signed release from the subject individual. | Proposed § 73.56(m)(2) would enhance the current requirement for the disclosure of relevant information to licensees, applicants, and C/Vs, and their authorized representatives who have a legitimate need for the information and a signed release from an individual who is seeking UAA under this part. This proposed provision would be added to further clarify current § 73.56 requirements because some licensees have misinterpreted the current provision as prohibiting the release of information to C/Vs who have licensee-approved authorization programs and require such information in determining |

| | | |
|---|---|---|
| held in confidence | (m)(4) A licensee's, applicant's, or C/V's contracts with any individual or organization who collects and maintains personal information that is relevant to an unescorted access authorization determination must require that such records be maintained as proprietary information, as required under 10 CFR 2.390, except as provided in paragraphs (m)(1) through (m)(3) of this section. | Proposed § 73.56(m)(4) would require that a licensee's, applicant's, or C/V's contracts with any individual or organization who collects and maintains personal information that is relevant to a UAA determination must require that such records be maintained in confidence, as required under 10 CFR 2.390. The paragraph would make an exception for the disclosure of information to the individuals identified in § 73.56(m)(1) through (m)(3). This paragraph would be added to ensure that entities who collect and maintain personal information use and maintain those records with the highest regard for individual privacy. |
| | | |

| | | |
|---|---|---|
| | appendix A to this part. Footnote: 2. Notifications to the NRC for the declaration of an emergency class shall be performed in accordance with § 50.72 of this chapter. | especially if this event is the opening action on an ineffectively coordinated multiple-target attack. Such notice may permit other licensees to escalate to a higher protective level in advance of an attack. The Commission would expect licensees to notify the NRC Operations Center as soon as possible after they notify local law enforcement agencies, but within 15 minutes The Commission may consider the applicability of this requirement to other types of licensees in future rulemaking. |

| | | |
|---|---|---|
| (a)(3) The licensee shall, upon request to the NRC, maintain an open and continuous communication channel with the NRC Operations Center. | (e)(3) For events reported under paragraph (a) of this section, the licensee may be requested by the NRC to maintain an open, continuous communication channel with the NRC Operations Center, once the licensee has completed other required notifications under this section, § 50.72 of this chapter, or Appendix E of part 50 of this chapter and any immediate actions to stabilize the plant. When established, the continuous communications channel shall be staffed by a knowledgeable individual | This requirement would be retained and revised into three separate requirements. The first sentence would be reworded to reflect the renumbered event reports under this section. For the 15-minute reports, the paragraph would indicate that a licensee may be requested to establish a "continuous communications channel" following the initial 15-minute notification. The establishment of a continuous communications channel would not supercede current emergency |

| | | |
|---|---|---|
| (a)(5) The revised report must replace the previous report; the update must be a complete entity and not contain only supplementary or revised information. | (g)(10) The revised report must replace the previous report; the update must be complete and not be limited to only supplementary or revised information. | This requirement would be renumbered and retained with minor grammatical changes. |
| (a)(5) Each licensee shall maintain a copy of the written report of an event submitted under this section as record for a period of three years from the date of the report. | (g)(11) Each licensee shall maintain a copy of the written report of an event submitted under this section as record for a period of three (3) years from the date of the report. | This requirement would be renumbered and retained with minor revision by adding "(3)" after "three" [years]. |
| (e) Duplicate reports are not required for events that are also reportable in accordance with §§50.72 and 50.73 of this chapter. | (h) Duplicate reports are not required for events that are also reportable in accordance with §§ 50.72 and 50.73 of this chapter. | This requirement would be retained and be renumbered. |

| | | |
|---|---|---|
| Appendix B, Introduction, Paragraph 1: Security personnel who are responsible for the protection of special nuclear material on site or in transit and for the protection of the facility or shipment vehicle against radiological sabotage should, like other elements of the physical security system, be required to meet minimum criteria to ensure that they will effectively perform their assigned security-related job duties. | A.1. The licensee shall ensure that all individuals who are assigned duties and responsibilities required to prevent significant core damage and spent fuel sabotage, implement the Commission approved security plans, licensee response strategy, and implementing procedures, meet minimum training and qualification requirements to ensure each individual possess the knowledge, skills, and abilities required to effectively perform the assigned duties and responsibilities. | This requirement would retain the requirement for security personnel to meet minimum criteria to ensure that they will effectively perform their assigned security-related job duties. The phrase "security personnel" would be replaced with the phrase "all individuals" to describe the Commission determination that any individual who is assigned to perform a security function must be trained and qualified to effectively perform that security function. The phrase "on site or in transit and for the |

| | | |
|---|---|---|
| | | individual possess the knowledge, skills, and abilities required to effectively perform the assigned duties and responsibilities" to describe the Commission determination that minimum training and qualification requirements are met to provide assurance that assigned individuals possess the knowledge, skills, and abilities that are required to effectively perform the assigned function. |

| | | |
|---|---|---|
| Appendix B, Paragraph I.C. Subsequent to this medical examination, guards, armed response personnel, armed escorts and other armed security force members shall demonstrate physical fitness for assigned security job duties by performing a practical physical exercise program within a specific time period. | B.4.b. Before assignment, armed members of the security organization shall demonstrate physical fitness for assigned duties and responsibilities by performing a practical physical fitness test. | This medical examination and physical fitness requirement would be retained. The phrase "guards, armed response personnel, armed escorts and other armed security force members" would be replaced with the phrase "armed members of the security organization" for consistency with terminology used in the proposed rule. The phrase "security job duties would be replaced with the phrase "assigned duties and responsibilities" for consistency with terminology used in the proposed rule. |

| | | |
|---|---|---|
| Appendix B, Paragraph II. A. Training Requirements - Each individual who requires training to perform assigned security - related job tasks or job duties as identified in the licensee physical security or contingency plans shall, prior to assignment, be trained to perform these tasks and duties in accordance with the licensee or licensee's agent's documented training and qualification plan. | C.3.a. Licensees shall demonstrate response capabilities through a performance evaluation program as described in Appendix C to this part. | This requirement would be based on the current Appendix B, Paragraph II.A.5. Due to changes in the threat environment, the requirement would specify that the licensee develop and follow a performance evaluation program designed to demonstrate the effectiveness of the onsite response capabilities. |

| | | |
|---|---|---|
| Appendix B, Paragraph II. A.<br><br>Training Requirements - Each individual who requires training to perform assigned security - related job tasks or job duties as identified in the licensee physical security or contingency plans shall, prior to assignment, be trained to perform these tasks and duties in accordance with the licensee or licensee's agent's documented training and qualification plan. | C.3.b. The licensee shall conduct drills and exercises in accordance with Commission approved security plans, licensee protective strategy, and implementing procedures. | This requirement would be based on the current Appendix B, Paragraph II.A.5. Due to changes in the threat environment, the requirement would specify that the licensee conduct drills and exercises to demonstrate the effectiveness of security plans, licensee protective strategy, and implementing procedures. |

| | | |
|---|---|---|
| Appendix B, Paragraph II. A.<br><br>Training Requirements - Each individual who requires training to perform assigned security - related job tasks or job duties as identified in the licensee physical security or contingency plans shall, prior to assignment, be trained to perform these tasks and duties in accordance with the licensee or licensee's agent's documented training and qualification plan. | C.3.b.(2) Tabletop exercises may be used to supplement drills and exercises to accomplish desired training goals and objectives. | This requirement would be based on the current Appendix B, Paragraph II.A. Due to changes in the threat environment, the requirement would convey the Commission view that licensees may use tabletop exercises to supplement drills and exercises as a means of achieving training goals and objectives. |
| | D. Duty qualification and requalification | This new header would be added for formatting purposes. The word "duty" would be used to clarify that the following sections relate to non-weapons training topics. |

| | | |
|---|---|---|
| Appendix B, Paragraph IV. Qualification firing for the handgun and the rifle must be for daylight firing, and each individual shall perform night firing for familiarization with assigned weapon(s). | F.4.c. Annual tactical qualification course. Qualifying score must be an accumulated total of 80 percent of the maximum obtainable score. | This requirement would combine the current qualification requirements in Appendix B, Paragraph IV.A., B., and C. In the proposed rule, the annual tactical course of fire would be developed and implemented to simulate the licensee protective strategy in accordance with the Commission approved training and qualification plan. Licensees would not be not required to include every aspect of its site protective strategy into one tactical course of fire. Instead, licensees should consider periodically |

| | | |
|---|---|---|
| Appendix B, Paragraph I.C. The physical fitness qualification of each guard, armed response person, armed escort, and other security force member shall be documented...<br><br>Appendix B, Paragraph I.C. The licensee shall retain this documentation as a record for three years from the date of each qualification.<br><br>Appendix B, Paragraph I.E. The licensee shall document each individual's physical requalification and shall retain this documentation of | H.2. The licensee shall retain each individual's initial qualification record for three (3) years after termination of the individual's employment and shall retain each re-qualification record for three (3) years after it is superceded. | This requirement would combine all record retention requirements currently in Appendix B. |

| | | |
|---|---|---|
| | I. Audits and reviews. | This heading would be added to ensure consistency with the structure of the appendix. |
| | The licensee shall review the Commission approved training and qualification plan in accordance with the requirements of § 73.55(n). | This requirement would be added for consistency with audit and review requirements of the proposed 10 CFR 73.55(n). |
| Definitions | J. Definitions | This heading would be brought forward from the current rule and would be renumbered accordingly. |
| Terms defined in Parts 50, 70, and 73 of this chapter have the same meaning when used in this appendix. | Terms defined in Parts 50, 70, and 73 of this chapter have the same meaning when used in this appendix. | This requirement would be brought forward from the current rule and would be renumbered accordingly. |

| | | |
|---|---|---|
| 2.a. Identification of those events that will be used for signaling the beginning or aggravation of a safeguards contingency according to how they are perceived initially by licensee's personnel. | (d)(3)(i) Identify the types of events that signal the beginning or initiation of a safeguards contingency event. | This requirement would be retained with editorial changes. The phrase "according to how they are perceived initially by licensee's personnel" would be deleted because the concept of "perceived" is captured through "assessment." |
| Introduction: The goals of licensee safeguards contingency plans...are:<br><br>(2) to provide predetermined, structured responses by licensees to safeguards contingencies, | (d)(3)(ii) Provide predetermined and structured responses to each type of postulated event. | This requirement would be retained with editorial changes. The phrase "safeguards contingencies" has been replaced with "each type of postulated event" to include a wider range of potential events. |
| 2.b. Definition of the specific objective to be accomplished relative to each identified event. | (d)(3)(iii) Define specific goals and objectives for response to each postulated event. | This requirement would be retained with editorial changes. The word "goals" would be added for consistency with the proposed Paragraph (a)(3). |

(5) * * *

(ii) Storage of spent fuel must be within a protected area, in accordance with § 73.55(e) of this chapter, but need not be within a separate vital area. Existing protected areas may be expanded or new protected areas added for the purpose of storage of spent fuel in accordance with this general license.

(iii) For purposes of this general license, personnel searches required by § 73.55(h) of this chapter before admission to a new protected area may be performed by physical pat-down searches of persons in lieu of firearms and explosives detection equipment.

check term being used ?

(iv) The observational capability required by § 73.55(i)(7) of this chapter as applied to a new protected area may be provided by a guard or watchman on patrol in lieu of closed circuit television.

(v) For the purpose of this general license, the licensee is exempt from §§ 73.55(k)(2) and 73.55(k)(7)(ii) of this chapter.

* * * * *

PART 73 - PHYSICAL PROTECTION OF PLANTS AND MATERIALS

7. The authority citation for Part 73 is revised to read as follows:

capable of facilitating timely evaluation of the detected unauthorized activities before completed penetration of the protected area perimeter barrier.

(ii) Assessment equipment in the isolation zone must provide real-time and play-back/recorded video images in a manner that allows timely evaluation of the detected unauthorized activities before and after each alarm annunciation.

(iii) Parking facilities, storage areas, or other obstructions that could provide concealment or otherwise interfere with the licensee's capability to meet the requirements of paragraphs (e)(5)(i)(A) and (B) of this section, must be located outside of the isolation zone.

(6) Protected Area.

(i) The protected area perimeter must be protected by physical barriers designed and constructed to meet Commission requirements and all penetrations through this barrier must be secured in a manner that prevents or delays, and detects the exploitation of any penetration.

(ii) The protected area perimeter physical barriers must be separated from any other barrier designated as a vital area physical barrier, unless otherwise identified in the approved physical security plan.

(iii) All emergency exits in the protected area must be secured by locking devices that allow exit only, and alarmed.

the central alarm station, must be provided protection equivalent to vital equipment and located within a vital area.

(iv) Vital equipment that is undergoing maintenance or is out of service, or any other change to site conditions that could adversely affect plant safety or security, must be identified in accordance with § 73.58, and adjustments must be made to the site protective strategy, site procedures, and approved security plans, as necessary.

(v) The licensee shall protect all vital areas, vital area access portals, and vital area emergency exits with intrusion detection equipment and locking devices. Emergency exit locking devices shall be designed to permit exit only.

(vi) Unoccupied vital areas must be locked.

(8) Vehicle Barrier System. The licensee must:

(i) Prevent unauthorized vehicle access or proximity to any area from which any vehicle, its personnel, or its contents could disable the personnel, equipment, or systems necessary to meet the performance objective and requirements described in paragraph (b).

(ii) Limit and control all vehicle approach routes.

(iii) Design and install a vehicle barrier system, to include passive and active barriers, at a stand-off distance adequate to protect personnel, equipment, and systems against the design basis threat.

(C) Implement compensatory measures upon discovery or suspicion that any access control device may have been compromised. Compensatory measures must remain in effect until the compromise is corrected.

(D) Retrieve, change, rotate, deactivate, or otherwise disable access control devices that have been, or may have been compromised.

(E) Retrieve, change, rotate, deactivate, or otherwise disable all access control devices issued to individuals who no longer require unescorted access to the areas for which the devices were designed.

(7) Visitors.

(i) The licensee may permit escorted access to the protected area to individuals who do not have unescorted access authorization in accordance with the requirements of § 73.56 and part 26 of this chapter. The licensee shall:

(A) Implement procedures for processing, escorting, and controlling visitors.

(B) Confirm the identity of each visitor through physical presentation of an identification card issued by a recognized local, state, or Federal Government agency that includes a photo or contains physical characteristics of the individual requesting escorted access.

(7) Vehicle search checkpoints must be equipped with video surveillance equipment that must be monitored by an individual capable of initiating and directing a timely response to unauthorized activity.

(8) Exceptions to the search requirements of this section must be identified in the approved security plans.

(submitted to the Commission for prior review and approval and must be

(i) Vehicles and items that may be excepted from the search requirements of this section must be escorted by an armed individual who is trained and equipped to observe offloading and perform search activities at the final destination within the protected area.

(ii) To the extent practicable, items excepted from search must be off loaded only at specified receiving areas that are not adjacent to a vital area.

(iii) The excepted items must be searched at the receiving area and opened at the final destination by an individual familiar with the items.

(i) Detection and Assessment Systems.

(1) The licensee shall establish and maintain an intrusion detection and assessment system that must provide, at all times, the capability for early detection and assessment of unauthorized persons and activities.

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

(iii) The licensee shall conduct random patrols of areas containing unirradiated MOX fuel assemblies to ensure the integrity of barriers and locks, deter unauthorized activities, and to identify indications of tampering.

(iv) Locks, keys, and any other access control device used to secure equipment and power sources required for the movement of unirradiated MOX fuel assemblies or openings to areas containing unirradiated MOX fuel assemblies must be controlled by the security organization.

(v) Removal of locks used to secure equipment and power sources required for the movement of unirradiated MOX fuel assemblies or openings to areas containing unirradiated MOX fuel assemblies must require approval by both the on-duty security shift supervisor and the operations shift manager.

(A) At least one armed security officer shall be present to observe activities involving the movement of unirradiated MOX fuel assemblies before the removal of the locks and providing power to equipment required for the movement or handling of unirradiated MOX fuel assemblies.

(B) At least one armed security officer shall be present at all times until power is removed from equipment and locks are secured.

(C) Security officers shall be trained and knowledgeable of authorized and unauthorized activities involving unirradiated MOX fuel assemblies.

(5) At least one armed security officer shall be present and shall maintain constant surveillance of unirradiated MOX fuel assemblies when the assemblies are not located in the spent fuel pool or reactor.

(6) The licensee shall maintain at all times the capability to detect, assess, intercept, challenge, delay, and neutralize threats to unirradiated MOX fuel assemblies in accordance with the requirements of this section.

(m) Digital Computer and Communication Networks.

(1) The licensee shall implement a cyber-security program that provides high assurance that computer systems, which if compromised, would likely adversely impact safety, security, and emergency preparedness, are protected from cyber attacks.

(i) The licensee shall describe the cyber-security program requirements in the approved security plans.

(ii) The licensee shall incorporate the cyber-security program into the onsite physical protection program.

(iii) The cyber-security program must be designed to detect and prevent cyber attacks on protected computer systems.

(2) Cyber-security Assessment. The licensee shall implement a cyber-security assessment program to systematically assess and manage cyber risks.

(t) Alternative Measures

(1) The Commission may authorize an applicant or licensee to provide a measure for protection against radiological sabotage other than one required by this section if the applicant or licensee demonstrates that:

(i) The measure meets the same performance objective and requirements as specified in paragraph (b) of this section and

(ii) The proposed alternative measure provides protection against radiological sabotage or theft of unirradiated MOX fuel assemblies, equivalent to that which would be provided by the specific requirement for which it would substitute.

(2) The licensee shall submit each proposed alternative measure to the Commission for review and approval in accordance with § 50.4 and § 50.90 before implementation.

(3) The licensee shall submit a technical basis for each proposed alternative measure, to include any analysis or assessment conducted in support of a determination that the proposed alternative measure provides a level of protection that is at least equal to that which would otherwise be provided by the specific requirement of this section.

(4) Alternative Vehicle Barrier Systems. In the case of alterative vehicle barrier systems required by § 73.55(e)(8), the licensee shall demonstrate that:

(i) the alternative measure provides substantial protection against a vehicle bomb, and



Also, delete next section (ii).

(ii) Any individual whose assigned duties and responsibilities permit the individual to take actions by electronic means, either on site or remotely, that could adversely impact a licensees or applicants operational safety, security, or emergency response capabilities; and

(iii) Any individual who has responsibilities for implementing a licensee's or applicant's protective strategy, including, but not limited to, armed security force officers, alarm station operators, and tactical response team leaders; and

(iv) The licensee's, applicant's, or C/V's reviewing official.

(2) At the licensee's, applicant's, or C/V's discretion, other individuals who are designated in access authorization program procedures may be subject to an authorization program that meets the requirements of this section.

(c) General performance objective. Access authorization programs must provide high assurance that the individuals who are specified in paragraph (b)(1), and, if applicable, (b)(2) of this section are trustworthy and reliable, ~~and~~ such that they do not constitute an unreasonable risk to public health and safety or the common defense and security, including the potential to commit radiological sabotage.

(d) Background investigation. In order to grant unescorted access authorization to an individual, the licensees, applicants, and C/Vs specified in paragraph (a) of this section shall ensure that the individual has been subject to a background investigation. The background investigation must include, but is not limited to, the following elements:

(f) Behavioral observation. Access authorization programs must include a behavioral observation element that is designed to detect 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.

(1) The licensees, applicants, and C/Vs specified in paragraph (a) of this section shall ensure that the individuals specified in paragraph (b)(1) and, if applicable, (b)(2) are subject to behavioral observation.

(2) Behavioral observation must be conducted by the individuals specified in paragraph (b)(1) and, if applicable, (b)(2). The licensees, applicants, and C/Vs specified in paragraph (a) of this section shall ensure that individuals who are subject to this section successfully complete behavioral observation training.

(i) Behavioral observation training must be completed before the licensee, applicant, or C/V grants an initial unescorted access authorization, as defined in paragraph (h)(5) of this section, and must be current before the licensee, applicant, or C/V grants an unescorted access authorization update, as defined in paragraph (h)(6) of this section, or an unescorted access authorization reinstatement, as defined in paragraph (h)(7) of this section;

(ii) Individuals shall complete refresher training on a nominal 12-month frequency, or more frequently where the need is indicated. Individuals may take and pass a comprehensive examination that meets the requirements of paragraph (f)(2)(iii) of this section in lieu of completing annual refresher training;

(iii) Individuals shall demonstrate the successful completion of behavioral observation training by passing a comprehensive examination that addresses the knowledge and abilities necessary to detect behavior or activities that have the potential to 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. Remedial training and re-testing are required for individuals who fail to satisfactorily complete the examination.

(iv) Initial and refresher training may be delivered using a variety of media (including, but not limited to, classroom lectures, required reading, video, or computer-based training systems). The licensee, applicant, or C/V shall monitor the completion of training.

(3) Individuals who are subject to an authorization program under this section shall report to the reviewing official any concerns arising from behavioral observation, including, but not limited to, concerns related to any questionable behavior patterns or activities of others.

Licensees shall not take action against individuals for false reporting and other abuses of this requirement.

(g) Arrest reporting. Any individual who has applied for or is maintaining unescorted access authorization under this section shall promptly report to the reviewing official any formal action(s) taken by a law enforcement authority or court of law to which the individual has been subject, including an arrest, an indictment, the filing of charges, or a conviction. On the day that the report is received, the reviewing official shall evaluate the circumstances related to the formal action(s) and determine whether to grant, maintain, administratively withdraw, deny, or unfavorably terminate the individual's unescorted access authorization.

(h) Granting unescorted access authorization. The licensees, applicants, and C/Vs specified in paragraph (a) of this section shall implement the requirements of this paragraph for

been provided to the reviewing official and he or she determines that the accumulated information supports a positive finding of trustworthiness and reliability.

(9) Unescorted access for NRC-certified personnel. The licensees and applicants specified in paragraph (a) of this section shall grant unescorted access to all individuals who have been certified by the Commission as suitable for such access including, but not limited to, contractors to the NRC and NRC employees.

(10) Access prohibited. Licensees and applicants may not permit an individual, who is identified as having an access-denied status in the information sharing mechanism required under paragraph (o)(6) of this section, or has an access authorization status other than favorably terminated, to enter any nuclear power plant protected area, vital area, under escort or otherwise, or take actions by electronic means that could impact the licensee's operational safety, security, or emergency response capabilities, under supervision or otherwise, except if, upon evaluation, the reviewing official determines that such access is warranted. Licensees and applicants shall develop reinstatement review procedures for assessing individuals who have been in an access-denied status.

(i) Maintaining access authorization.

(1) Individuals may maintain unescorted access authorization under the following conditions:

(i) The individual remains subject to a behavioral observation program that complies with the requirements of paragraph (f) of this section;

(v) An evaluation of character and reputation.

(2) Authorization program personnel. Licensees, applicants, and C/Vs shall ensure that any individual who evaluates personal information for the purpose of processing applications for unescorted access authorization including, but not limited to a clinical psychologist of psychiatrist who conducts psychological assessments under paragraph (e) of this section; has unfettered access to the files, records, and personal information associated with individuals who have applied for 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 authorization program that meets requirements of this section; or

(ii) The licensee, applicant, or C/V determines that the individual is trustworthy and reliable based upon an evaluation that meets the requirements of paragraphs (d)(1) through (d)(5) and (e) of this section and a local criminal history review and evaluation from the State of the individual's permanent residence.

(l) Review procedures. Each licensee, applicant, and C/V who is implementing an authorization program under this section shall include a procedure for the review, at the request of the affected individual, of a denial or unfavorable termination of unescorted access authorization which adversely affects employment. The procedure must require that the individual is informed of the grounds for the denial or unfavorable termination and allow the individual an opportunity to provide additional relevant information, and provide an opportunity

(v) The presiding officer in a judicial or administrative proceeding that is initiated by the subject individual;

(vi) Persons deciding matters under the review procedures in paragraph (k) of this section; and

(vii) Other persons pursuant to court order.

(2) Personal information that is collected under this section must be disclosed to other licensees, applicants, and C/Vs, or their authorized representatives, who are legitimately seeking the information for unescorted access authorization determinations under this section and who have obtained a signed release from the subject individual.

(3) Upon receipt of a written request by the subject individual or his or her designated representative, the licensee, applicant, or C/V possessing such records shall promptly provide copies of all records pertaining to a denial or unfavorable termination of the individual's unescorted access authorization.

(4) A licensee's, applicant's, or C/V's contracts with any individual or organization who collects and maintains personal information that is relevant to an unescorted access authorization determination must require that such records be maintained as proprietary information, as required under 10 CFR 2.390, except as provided in paragraphs (m)(1) through (m)(3) of this section.

confidentially held

VI. Nuclear Power Reactor Training and Qualification Plan.

A. General requirements and introduction.

1. The licensee shall ensure that all individuals who are assigned duties and responsibilities required to prevent significant core damage and spent fuel sabotage, implement the Commission approved security plans, licensee response strategy, and implementing procedures, meet minimum training and qualification requirements to ensure each individual possess the knowledge, skills, and abilities required to effectively perform the assigned duties and responsibilities.

2. To ensure that those individuals who are assigned to perform duties and responsibilities required for the implementation of the Commission approved security plans, licensee response strategy, and implementing procedures are properly suited, trained, equipped, and qualified to perform their assigned duties and responsibilities, the Commission has developed minimum training and qualification requirements that must be implemented through a Commission approved training and qualification plan.

3. The licensee shall establish, maintain, and follow a Commission approved training and qualification plan, describing how the minimum training and qualification requirements set forth in this appendix will be met, to include the processes by which all members of the security organization, will be selected, trained, equipped, tested, and qualified.

4. Each individual assigned to perform security program duties and responsibilities required to effectively implement the Commission approved security plans, licensee protective

(1) Possess a high school diploma or pass an equivalent performance examination designed to measure basic mathematical, language, and reasoning skills, abilities, and knowledge, required to perform security duties and responsibilities.

(2) Have attained the age of 21 for an armed capacity or the age of 18 for an unarmed capacity; and

(3) An unarmed individual assigned to the security organization may not have any felony convictions that reflect on the individual's reliability.

b. The qualification of each individual to perform assigned duties and responsibilities must be documented by a qualified training instructor and attested to by a security supervisor.

2. Physical qualifications.

a. General physical qualifications.

(1) Individuals whose duties and responsibilities are directly associated with the effective implementation of the Commission approved security plans, licensee protective strategy, and implementing procedures, may not have any physical conditions that would adversely affect their performance.

(2) Armed and unarmed members of the security organization shall be subject to a physical examination designed to measure the individual's physical ability to perform assigned

(2) Firearms maintenance procedures that include cleaning schedules and cleaning requirements.

(3) Program activity documentation.

(4) Control and Accountability (Weapons and ammunition).

(5) Firearm storage requirements.

(6) Armorer certification.

H. Records.

1. The licensee shall retain all reports, records, or other documentation required by this appendix in accordance with the requirements of § 73.55(r).

2. The licensee shall retain each individual's initial qualification record for three (3) years after termination of the individual's employment and shall retain each re-qualification record for three (3) years after it is superseded.

3. The licensee shall document data and test results from each individual's suitability, physical, and psychological qualification and shall retain this documentation as a record for three years from the date of obtaining and recording these results.

I. Audits and reviews.