[7590-01-P]

NUCLEAR REGULATORY COMMISSION

10 CFR Parts 50, 52, and 73

RIN 3150 - AH92

Security Assessment Requirements for New Nuclear Power Reactor Designs

AGENCY: Nuclear Regulatory Commission.

ACTION: Supplemental proposed rule.

SUMMARY: The Nuclear Regulatory Commission (NRC or Commission) is proposing to amend its regulations by adding security design assessment requirements for future applicants for a construction permit, operating license, standard design approval, design certification, manufacturing license, or combined license. The proposed amendments would require applicants to assess specific security design features that would be incorporated into the facility design (including site layout) to support enhanced security effectiveness. The proposed amendments are needed to ensure that security design features are assessed early in the design and regulatory review process, and not later, when it could be more difficult to incorporate the features. Resolution of security design issues at the early stage of the regulatory review process would result in a more robust security posture requiring less reliance on operational security programs.

DATES: Submit comments on the rule by (INSERT DATE 75 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*). Submit comments on the information collection aspects of this rule by (INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*). Comments received after the above dates will be considered if it is practical to do so, but assurance of consideration cannot be given to comments received after these dates.

ADDRESSES: You may submit comments by any of the one of the following methods. Please include the number RIN 3150-AH92 in the subject line of your comments. Comments on rulemakings submitted in writing or in electronic form will be made available for public inspection. Because your comments will not be edited to remove any identifying or contact information, the NRC cautions you against including personal information such as social security numbers and birth dates in your submission.

Mail comments to the Secretary, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, ATTN: Rulemakings and Adjudications Staff.

Email comments to SECY@nrc.gov. If you do not receive a reply email confirming that we have received your comments, contact us directly at (301) 415-1966. You may also submit comments via the NRC's rulemaking Web site at http://ruleforum.llnl.gov. Address questions about our rulemaking Web site to Carol Gallagher at (301) 415-5905; email CAG@nrc.gov. Comments can also be submitted via the Federal eRulemaking Portal at http://www.regulations.gov.

Hand deliver comments to 11555 Rockville Pike, Rockville, Maryland 20852, between 7:30 am and 4:15 pm Federal workdays. (telephone (301) 415-1966).

Fax comments to the Secretary, U.S. Nuclear Regulatory Commission at (301) 415-1101.

Publicly available documents related to this rulemaking may be viewed electronically on the public computers located at the NRC's Public Document Room (PDR), O1 F21, One White Flint North, 11555 Rockville Pike, Rockville, Maryland. The PDR reproduction contractor will copy documents for a fee. Selected documents, including comments, may be viewed and downloaded electronically via the NRC rulemaking Web site at http://ruleforum.llnl.gov.

Publically available documents created or received at the NRC after November 1, 1999, are available electronically at the NRC's Electronic Reading Room at

http://www.nrc.gov/reading-rm/adams.html. From this site, the public can gain entry into the NRC's Agencywide Document Access and Management System (ADAMS), which provides text and image files of the NRC's public documents. If you do not have access to ADAMS, contact the NRC PDR Reference staff at (800) 397-4209 or (301) 415-4737 or by email to PDR@nrc.gov.

You may submit comments on the information collections made by the methods indicated in the "Paperwork Reduction Act Statement."

FOR FURTHER INFORMATION CONTACT: Stewart Schneider, Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, telephone (301) 415-4123, email SXS4@nrc.gov; or Larry C. Harris, Office of Nuclear Security and Incident Response, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, telephone (301) 415-5072, email LCH1@nrc.gov.

SUPPLEMENTARY INFORMATION:

I. Background

Since the events of September 11, 2001, the NRC has assessed potential threats and their possible impacts to nuclear power reactors and has required upgrades of physical security measures and mitigative strategies at the Nation's fleet of operating power reactors. For new nuclear power reactors, the NRC determined that applicants for a construction permit, operating license, standard design approval, design certification, manufacturing license, or combined license should be required to assess the design and incorporate specific security design features to support security effectiveness. The Commission views resolution of security design issues at the early stage of the design and regulatory review process as an activity that would result in a design that inherently provides a more robust security posture and requires less reliance on security operational programs. Experience has shown that a specific design feature that might be advantageous for security could be difficult to incorporate into the facility design once the design is completed or the facility is built.

The Commission is publishing this proposed rule as a supplement to the proposed rule, "Power Reactor Security Requirements," published on XX XX, 2006 (XX FR XXXX) that

would amend the current security regulations and add new security requirements pertaining to existing and new nuclear power reactors. Among other changes, the September 2006 proposed rule would update requirements for physical security plans, training and qualification plans, and safeguards contingency plans to reflect experience gained since September 11, 2001. These requirements are collectively referred to later in this notice as "security operational programs." In particular, the September 2006 proposed rule would require that the physical protection program must be designed to detect, delay, assess, and respond to threats up to and including the design basis threat (DBT) of radiological sabotage (the DBT as defined in Title 10, Section 73.1, "Purpose and Scope," of the *Code of Federal Regulations* (10 CFR 73.1) is also being revised by a separate rulemaking (70 FR 67380; November 7, 2005)). Furthermore, the September 2006 proposed rule would require the development of guidance and strategies to mitigate the circumstances associated with loss of large areas of the plant due to explosions or fire. The requirements in this proposed rule supplement the provisions of the September 2006 proposed rule by requiring applicants for a construction permit, operating license, standard design approval, design certification, manufacturing license, or combined license for new nuclear power reactors to conduct a security assessment and include it with their applications. The definitions proposed in the September 2006 proposed rule, such as "target set,"[1] apply to this rulemaking as well. As a result, the enclosed notice contains the entire text for the rule under 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage," as it is being proposed in the Federal Register

---

[1]Target set is defined in the September 2006 proposed rule as: the combination of equipment or operator actions, that, if all are prevented from performing their intended safety function or prevented from being accomplished, would likely result in significant core damage (e.g., non-incipient, non-localized fuel melting, and/or core disruption) barring extraordinary action by plant operators. A target set with respect to spent fuel sabotage is draining the spent fuel pool leaving the spent fuel uncovered for a period of time, allowing spent fuel heat up and the associated potential for release of fission products.

(in XX XX, 2006), with the proposed addition of paragraph (a)(7) for security assessments. No other changes are being proposed to 10 CFR 73.55 in this supplemental proposed rule.

In a separate regulatory action, the NRC previously published a proposed rule (71 FR 12782; March 13, 2006) that would substantially revise and reformat 10 CFR Part 52, "Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants," and that make numerous conforming changes in other parts. The new security assessment requirement is being proposed with respect to the existing 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," and 10 CFR Part 52 requirements. It is the Commission's intent that when this supplemental proposed rule and the proposed revisions to 10 CFR Part 52 are final, the appropriate conforming changes would be made to the security assessment rule to reflect the amended 10 CFR Part 52 with respect to such matters as the numbering of the content of application sections.

II. Rulemaking Initiation

In 2003, the NRC staff presented the Commission with various options for establishing security requirements for new power reactors and recommended requirements to incorporate security into the design at the design certification and combined license phases. Subsequently, in SECY-05-0120, "Security Design Expectations for New Reactor Licensing Activities," dated July 6, 2005 (ADAMS Accession No. ML051100233), the NRC staff proposed to initiate rulemaking to 10 CFR Parts 50 and 52, requiring applicants for new reactor licensing activities to submit a security assessment and target set analysis. In response to SECY-05-0120, the Commission issued on September 9, 2005, a staff requirements memorandum (SRM) (ADAMS Accession No. ML052520334), directing the staff, in part, to conduct a rulemaking to require applicants to submit a safety and security assessment.

The Commission decided to require a security assessment through a rule because requiring nuclear power plant designers to analyze and establish security design features at the early stage of the design and regulatory review process would improve the overall design resulting in a more robust and effective security posture. Also under this proposed requirement future applicants would have to perform a target set analysis that enables them to analyze, consider, and establish security design aspects of advanced features in security technology for mitigation, access control, physical security, barriers, and intrusion detection systems. This would include an analysis of design capability, redundancy, and placement.

III. Public Input to the Proposed Rule

The NRC conducted a public meeting on March 6, 2006, to obtain stakeholder input on the structure and scope of the security assessments for new nuclear power reactors. Stakeholder participants discussed their related activities and willingness to participate in the rulemaking process. On July 17, 2006, the NRC posted the draft rule language on its interactive rulemaking Web site located at http://ruleforum.llnl.gov to facilitate public input on the proposed rule. The NRC held an additional public meeting on July 25, 2006, to obtain stakeholder input on the draft rule language. Stakeholders sought clarification on wording of certain proposed provisions and were concerned about the impact on near-term combined license applications.

IV. Proposed Regulations

The proposed rule would require applicants for a construction permit, operating license, or standard design approval under 10 CFR Part 50 and applicants for a design certification, manufacturing license, or combined license under 10 CFR Part 52 to conduct a security

assessment and include it with their applications. The security assessment would be based on threat situations identified by the NRC and the physical protection objectives. The NRC's intent is that security be examined in a holistic manner considering the facility design (including the layout of the facility) and physical characteristics of the site. Under this proposed rule, part of the licensing basis for these structures, systems, and components would include their contribution to common defense and security.

The NRC recognizes that future power reactors could be made more secure through security design features that reduce the need for security operational programs and that could prevent the loss of safety systems and functions, perhaps reducing the need for mitigating strategies. Because this type of consideration for security best occurs while the design itself is being developed, requirements are proposed for applicants in the design phase. Furthermore, other parts of the security assessment would be deferred until a site or a licensee is identified. Accordingly, applicants would have to assess (within the scope of design being addressed at the particular stage of the regulatory process) security design features for the protection of structures, systems, and components by:

(1) Identifying target sets;

(2) Applying a risk evaluation methodology;

(3) Using security assessment parameters to evaluate candidate security design features; and

(4) Using a systematic screening process to determine the practicability of these candidate security design features.

The systematic screening process would have to consider the impact on plant operations, security program implementation, and cost-effectiveness of the security design features. The applicant could make appropriate changes to the design or present an evaluation showing that implementation of the security design feature is not practicable. These could

include, for example, changing the location and design of access doors into plant equipment rooms to consider security functions as well as safety and operational aspects.

Furthermore, applicants would need to explain how the security design features are incorporated into the facility design (i.e., structures, systems, and components) and how they implement their security programs at the site (for layout of the vital areas, protected area and owner controlled area), provide or enhance the capability to protect the target sets against an adversary possessing the characteristics of the DBT, mitigate the effects of such an attack, or mitigate the effects of circumstances associated with loss of large areas of the facility due to explosions or fires. The Commission does not expect applicants to demonstrate that design features alone are sufficient to mitigate all such circumstances.

The NRC notes that an applicant may determine that certain scenarios may necessitate the consideration of features that are outside the scope of the security assessment being performed. Thus, the process includes provisions for the use of *security assessment parameters* to assess design features and, as needed, certain aspects to be recorded as unresolved and addressed by a future applicant who references the design and the assessment. These provisions would also apply when a feature is within the scope of the assessment being performed but its design is deferred to a future applicant who would have additional information to improve the security design feature. Ultimately, any security design issue identified by an assessment but not addressed by a security design feature at any application stage would be identified by a security assessment parameter and required to be addressed during the development of the security operational programs under the provisions of 10 CFR Part 73, “Physical Protection of Plants and Materials.”

Lastly, applicants would need to demonstrate that the practicable security design features that were identified under the proposed 10 CFR 73.62, “Security Assessment for Nuclear Power Plants,” were included in the security plans required by the proposed

10 CFR 73.55 and associated appendices. The security assessment submitted by the applicant will serve as one of the technical bases for evaluating the applicant's security program during the licensing phase. The NRC would require the applicant to incorporate the security design features identified in the assessment into the licensee's security plans. The approved security plans would be designated as a condition in the issued license. As a result, security design features and functions that were identified in the completed assessment and incorporated in the security plans would be subject to the formal change process as described in 10 CFR 50.54(p) and 10 CFR 50.90, "Application for Amendment of License or Construction Permit."

Any licensee must comply with the requirements under 10 CFR 73.55, to (1) detect, delay, assess, and respond to an attack against target sets of a nuclear power plant by an adversary possessing the characteristics of the DBT; (2) mitigate the effects of such an attack; and (3) mitigate the effects of circumstances associated with loss of large areas of the facility due to explosions or fires. The additional requirement that an application include a security assessment would ensure that the provisions under 10 CFR 73.55 are met.

Resolution of security design issues does not constitute final NRC approval of an applicant's overall security program. NRC review and approval of an applicant's security program would be required before issuing a combined license under 10 CFR Part 52, or an operating license under 10 CFR Part 50, for a specific site.

The Commission does not propose to require applicants to provide a security assessment if their reactor designs are in the design certification review process before the final rule is effective. However, the Commission encourages these applicants to conduct and submit a security assessment to the NRC. For example, since the applicant for the Economic Simplified Boiling Water Reactor (ESBWR) has already submitted its application for a design certification before the effective date of this final rule, it would be encouraged to conduct a security assessment to enhance their design. For the U.S. Evolutionary Power Reactor (EPR)

applicant, what would be expected with respect to a security assessment for the design certification stage would depend on when the application is submitted to the NRC. The NRC encourages this applicant to conduct a security assessment if their application is submitted before the effective date of the final rule. However, if the application is submitted after the effective date, a security assessment would need to be provided to the NRC that complies with final rule requirements. If an applicant voluntarily submits this assessment, the NRC would review it to ensure that the security design features identified and described are consistent with the Commission's security requirements. The Commission does not intend to require a security assessment for the existing design certifications approved in Appendices A through D in 10 CFR Part 52, nor would applicants who reference any of these already certified designs be required to make enhancements to features of those portions of the design that have been certified.

The NRC has taken several steps to keep stakeholders informed about the development of this proposed rule as a means of assisting potential applicants. First, a draft of the rule language was posted on the NRC's interactive rulemaking Web site and a public meeting held during the development of the proposed rule. The NRC staff is also working aggressively to develop draft regulatory guidance during the first calendar quarter of 2007 and to identify candidates for pilot activities before finalizing the rule. The Commission is aware that combined license applications may be submitted around the expected effective date for this final rule. However, potential near-term applicants (i.e., applications filed up to 6 months after the effective date of the rule) would have had the opportunity to review the proposed *Federal Register* document and the draft rule language on the NRC's rulemaking Web site. Thus, the Commission is proposing to phase-in compliance with the final rule. For combined license applications filed no later than 6 months after the effective date of the final rule, the Commission would not require that a security assessment be included with the application.

However, the applicant would be required to file the security assessment no later than 12 months after the effective date of the rule. Normally, an incomplete application would not be accepted for docketing. In this instance, because of the timing of the final security assessment rulemaking, the NRC believes it is reasonable to provide some time for the conduct of the security assessment and the filing of the security assessment part of the application. This process would allow the NRC staff to begin reviewing the application, while the applicant continues to prepare the security assessment. For these near-term applicants, a later filing of a completed security assessment will not delay the licensing review schedule for issuing the combined license. Thus, a filed application that the Commission determines is complete except for the lack of the security assessment would be considered complete and acceptable for docketing under 10 CFR 2.101, "Filing of Application." (As noted below in Section VI, the Commission is also interested in other approaches to deal with this issue).

V. Security Assessment Scope

The security assessment for new power reactors would be based on identified threats. The completed assessment would provide a description of the process to develop and identify target sets, including methodologies used to determine and group the target set equipment, methodologies used to perform the assessment, a list of security functions, the security design features incorporated into the design, the security assessment parameters, and the security assessment parameters to be considered at future design and construction stages as applicable. The scope of the assessment performed by an applicant would depend upon the particular stage of the application process and would determine the security design features to be incorporated into the facility design, site, and security operational programs (as applicable). A license application that incorporates by reference a construction permit, design certification,

or manufacturing license, would not be required to address the design of the facility or site within the scope of the previously completed assessment for the referenced permit, certification, or license. If an applicant references one of the four already certified designs, the assessment would not be intended to require enhancements to the portion of the design that has been certified.

The following discussion describes how the scope of the security assessment would vary depending on the particular stage of the application process in 10 CFR Parts 50 and 52.

1. Construction Permit (10 CFR Part 50). At the construction permit stage, an applicant would have selected a design and the site on which to build the plant. The scope of the assessment must include a description of the applicant's plan for conducting a security assessment that complies with the proposed 10 CFR 73.62 and describes the security design features incorporated into the final design of the site based on the design and site characteristics. Scenarios that necessitate evaluation of the security operational programs would be outside the scope of this assessment. Any security design issue identified but not addressed by a security design feature would be recorded as unresolved and addressed by a future applicant who uses the construction permit.

2. Operating License (10 CFR Part 50). Generally, the applicants for a construction permit and an operating license are the same entity. At the operating license stage, the applicant would have developed the security operational programs. The scope of the assessment must include (1) reference to the security assessment for the construction permit, (2) a description of how security design features left unresolved at the construction permit stage were resolved, and (3) scenarios that necessitate evaluation of the security operational programs. Ultimately, any security design issue identified by the assessment that is not

resolved by a security design feature would be identified by a security assessment parameter and must be resolved by the security operational programs.

3. Design Certification (10 CFR Part 52). At the design certification stage, the applicant would know the design but not the site or the security operational programs. The scope of the security assessment must include a description of the applicant's plan for conducting a security assessment that complies with the proposed 10 CFR 73.62 and describe the security design features incorporated into the design based on the scenarios evaluated by the assessment. Scenarios that necessitate evaluation of site characteristics and the security operational programs would be outside the scope of this assessment. However, the applicant may decide to assess the effectiveness of the plant's security design features at a hypothetical site or sites having characteristics that fall within a set of postulated site parameters (e.g., the location of transportation routes, heat sink, water access ways, and vehicle pathways). Any security design issue identified but not addressed by a security design feature would be recorded as unresolved and addressed by a future applicant who references the design certification.

4. Manufacturing License. An applicant for a manufacturing license who references a design certification for which a security assessment was done would know the design but not the site or the security operational programs. However, because the manufacturing license applicant would not change the information in the design certification, a security assessment would not be required at the manufacturing license stage. Any security design issue identified but not addressed by a security design feature at the design certification stage would continue to be recorded as unresolved and addressed by a future applicant who references the manufacturing license.

If the manufacturing license application proposes to use a custom design (i.e., not

reference a design certification), then the scope of the assessment would be the complete design. Any security design issue identified but not addressed by a security design feature would be recorded as unresolved and to addressed by a future applicant who references the manufacturing license.

5. Standard Design Approval. At the standard design approval stage, the applicant would know the design but not the site or the security operational programs. The application must include a description of the applicant's plan for conducting a security assessment that complies with the proposed 10 CFR 73.62 and describe the security design features incorporated into the design based on the scenarios evaluated by the assessment. Scenarios that necessitate evaluation of site characteristics and the security operational programs would be outside the scope of this assessment. However, the applicant may decide to assess the effectiveness of the plant's security design features at a hypothetical site or sites having characteristics that fall within a set of postulated security assessment parameters (e.g., the location of transportation routes, heat sink, water access ways, and vehicle pathways). Any security design issue identified but not addressed by a security design feature would be recorded as unresolved and addressed by a future applicant who uses the standard design approval, in developing its security operational program.

6. Combined License (10 CFR Part 52).

An applicant for a combined license who selects a plant design by referencing either a design certification or manufacturing license for which a security assessment was done, would know the design, the site, and the operational security program. The scope of the assessment must include (1) reference to the security assessment for either the design certification or

manufacturing license, (2) a description of how security design features left unresolved by the design certification or manufacturing license were addressed, and (3) scenarios that necessitate consideration of the site characteristics and the security operational programs. Ultimately, security design issues identified by this or a previous assessment which are not resolved by a security design feature would be identified by a security assessment parameter and must be resolved by the security operational programs.

If the combined license application proposes to use a custom design, then the scope of the security assessment would include a complete security assessment, including what would otherwise have been performed at the design certification stage, as described above. A combined license applicant referencing an already-certified design would not be required to make enhancements to the plant design within the scope of the design certification.

If the combined license application proposes to use a standard design approval, then the scope of the security assessment would include a complete security assessment, including what would otherwise have been performed at the design certification stage, as described above. A combined license applicant referencing an already-certified design would not be required to make enhancements to the plant design within the scope of the design certification.

VI. Request for Comment on Implementation of Proposed Requirements

The Commission is open to considering different approaches to implementing the proposed rule during the first year the final rule is effective and is seeking public comment on this matter. As discussed, the Commission is proposing additional time to achieve compliance for combined license applications with the proposed rule. The Commission believes that the implementation schedule would most concern applicants for a combined license because this category of applicants is most likely to file an application during the first year after the final rule

is effective. Other approaches are being considered for implementation during the first year.

For example, for an application filed no later than 6 months after the effective date of the final rule, the combined license applicant could be given the flexibility to include a simplified security assessment that delineated target sets and security assessment results. The Commission believes it is reasonable to expect these applicants to file a simplified assessment immediately after the effective date because they would be aware of the Commission's potential requirements—having had the opportunity to review this proposed rule, review the draft rule language on the NRC's interactive rulemaking Web site, and attend public meetings on the progress of this rulemaking. Furthermore, the Commission expects that the applications received in the first 6 months after the effective date of the rule would likely reference a certified design or one currently under review by the Commission for which a security assessment that conforms with the proposed rule was probably not performed. Thus, the filing of a simplified security assessment would ensure that the security design issues had been addressed with respect to the site design and security operational programs. However such a simplified assessment would be expected to also identify those aspects not presently considered and that must be addressed at a later stage. For applications filed 6 months to 1 year after the effective date of the final rule, the security assessment could be filed separately but it would have to be filed no later than 1 year after the effective date. In this case, the assessment would have to comply with the requirements of the proposed 10 CFR 73.62.

A different approach would be to encourage applicants who file no later than 6 months after the effective date of the rule to include a security assessment with their applications, but not make it a formal requirement. However, after 6 months, the applicant would have to meet all of the security assessment requirements under 10 CFR 73.62 and would have the flexibility to file the assessment separately from the application. The security assessment would have to be filed no later than 1 year after the effective date of the final rule. Finally, if the applicant

considers the implementation schedule for filing the security assessment too burdensome, the applicant can request that the Commission consider an exemption to the implementation schedule.

The Commission recognizes that developers of recent designs (such as the Advance Passive 1000 (AP1000) and ESBWR) have conducted some type of security assessment. Another approach the Commission is considering is to require combined license applicants who reference these designs to incorporate security design features (identified by those reviews) into their combined license designs.

The Commission requests specific public comments regarding these approaches and whether the contemplated periods of implementation are reasonable. The Commission is also soliciting public comments on other approaches for consideration and whether the Commission needs to provide similar flexibility to applicants for a design certification or manufacturing license.

VII. Section-by-Section Analysis

The Commission is proposing to amend 10 CFR 50.34, “Contents of Applications; Technical Information”; Appendices M, “Standardization of Design; Manufacture of Nuclear Power Reactors; Construction and Operation of Nuclear Power Reactors Manufactured Pursuant to Commission License,” and O, “Standardization of Design: Staff Review of Standard Designs,” to 10 CFR Part 50; 10 CFR 52.3, “Definitions”; 10 CFR 52.47, “Contents of Applications”; 10 CFR 52.54, “Issuance of Standard Design Certification”; 10 CFR 52.79, “Contents of Applications; Technical Information”: Appendices M, “Standardization of Design; Manufacture of Nuclear Power Reactors; Construction and Operation of Nuclear Power Reactors Manufactured Pursuant to Commission License,” and O, “Standardization of Design:

Staff Review of Standard Designs," to 10 CFR Part 52; 10 CFR 73.8, "Information Collection Requirements; OMB Approval"; and § 73.55. In addition, the Commission is adding a new 10 CFR 73.62. As noted earlier, these changes are proposed with respect to the current 10 CFR Parts 50 and 52.

Section 50.34—Contents of applications; technical information.

Paragraph (h) would be redesignated as paragraph (m), and paragraphs (i) through (l) would be reserved. A new 10 CFR 50.34(h), would then be added to require an application for a construction permit or an operating license to include a security assessment for the design of the facility and site. Paragraph (h)(1) would require that each application for a construction permit describe how the applicant will comply with 10 CFR 73.62 in completing the design of the nuclear power plant. It would also require the application to describe the applicant's plan for conducting a security assessment that complies with 10 CFR 73.62(d) and describe the security design features incorporated into the design of the site. In addition, paragraph (h)(2) would require that each application for an operating license contain a security assessment that complies with the requirements of 10 CFR 73.62.

Appendix M to 10 CFR Part 50—Standardization of Design: Manufacture of Nuclear Power Reactors: Construction and Operation of Nuclear Power Reactors Manufactured Pursuant to Commission License.

A new paragraph (4)(c) would be added to require that each application for a manufacturing license describe how the applicant will comply with 10 CFR 73.62 in completing the design of the nuclear power plant, including a description of the applicant's plan for

conducting a security assessment that complies with 10 CFR 73.62(d). Paragraph (4)(c) would also require the application to describe the security design features incorporated into the design of the facility.

Appendix O to 10 CFR Part 50—Standardization of Design: Staff Review of Standard Designs.

Paragraph (3) would be revised so that the submittal for review of the standard design must also include the applicable technical information required by 10 CFR 50.34(h).

Section 52.3—Definitions.

Paragraph (e) would be revised to require that all other terms in 10 CFR Part 50 also have the meanings set out in 10 CFR 73.2, “Definitions,” and 10 CFR 73.62, as applicable.

Section 52.47—Contents of applications.

Paragraphs (c) through (f) would be reserved. A new paragraph (g) would then be added to 10 CFR 52.47 to require that each application for a standard design certification contain a security assessment that complies with the requirements of 10 CFR 73.62. Paragraph (g) would also require that each application describe the security design features incorporated into the standard design certification.

Section 52.54—Issuance of standard design certification.

In 10 CFR 52.54, the current paragraph would be designated as paragraph (a). A new paragraph (b) would then be added to require that the design certification rule specify the site parameters, security design features, security assessment parameters, and any additional requirements of the design certification rule.

Section 52.79—Contents of applications; technical information.

Paragraphs (e) through (f) would be reserved. A new paragraph (g) would then be added to 10 CFR 52.79 to require that each application for a combined license contain a security assessment that complies with the requirements of 10 CFR 73.62. Paragraph (g) would also require the application to describe the security design features incorporated into the design of the nuclear power plant.

If the application references either a standard design certification rule under Subpart B, "Standard Design Certifications," of 10 CFR Part 52, or the use of a nuclear power reactor manufactured under a manufacturing license in Appendix M of 10 CFR Part 52, additional requirements would apply under paragraph (g)(1). Specifically–

The security assessment performed for the design certification or manufacturing license must be incorporated by reference into the application;

The application need not address the design of the plant within the scope of the design certification or manufacturing license; and

The application must identify the security functions, security design features, and security operational programs, and describe how security functions, not previously evaluated at the design stage, are addressed.

If the application references a design already certified by the Commission (Appendices A through D of 10 CFR Part 52), under paragraph (g)(2) the application would not be required to address the design of the plant within the scope of the design certification. However, it would be required to identify the security functions, security design features, and security operational programs, and describe how security functions, not previously evaluated at the design certification stage, are addressed.

Finally, paragraph (g)(3) would stipulate that if the application is filed no later than 6 months after the effective date of the final rule, the security assessment and any associated design changes may be filed no later than 12 months after the effective date of the final rule. In this case, a filed application that the NRC determines is complete except for the lack of the security assessment would be considered complete and acceptable for docketing under 10 CFR 2.101.

Appendix M to 10 CFR Part 52—Standardization of Design: Manufacture of Nuclear Power Reactors: Construction and Operation of Nuclear Power Reactors Manufactured Pursuant to Commission License.

A new paragraph (4)(c) would be added to require that each application for a manufacturing license describe how the applicant will comply with 10 CFR 73.62 in completing the design of the nuclear power plant, including a description of the applicant's plan for conducting a security assessment that complies with 10 CFR 73.62(d). Paragraph (4)(c) would also require the application to describe the security design features incorporated into the design of the facility.

Appendix O to 10 CFR Part 52—Standardization of Design: Staff Review of Standard Designs.

Paragraph (3) would be revised so that the submittal for review of the standard design must also include the applicable technical information required by 10 CFR 50.34(h).

Section 73.8—Information collection requirements: OMB approval.

This section would be revised to add the newly proposed 10 CFR 73.62 to the list of sections containing OMB approved information collection requirements.

Section 73.55—Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

The proposed rule related to power reactor security requirements published on **XX XX, 2006 [CITATION]** would revise 10 CFR 73.55 in its entirety. The bases for those proposed changes are explained in that proposed rule. In this supplemental proposed rule, the Commission proposes to modify the language in that proposed rule by adding a new paragraph (a)(7). The added provision would require an applicant for a license to operate a nuclear power reactor to include those design features, identified through the assessment process in 10 CFR 73.62`, into its security plans. This is the only change being made to 10 CFR 73.55 in this supplemental proposed rule.

Section 73.62—Security assessment for nuclear power plants.

A new 10 CFR 73.62 would be added to provide the requirements for the conduct and

content of a security assessment for nuclear power plants. Paragraph (a) would define three terms needed to implement the requirements under 10 CFR 73.62.

First a definition for *security design features* would designate the structures, systems, and components of a nuclear power plant and their layout that are relied upon to either: (1) detect, delay, assess, or respond to an attack against target sets of a nuclear power plant by an adversary possessing the DBT characteristics, (2) mitigate the effects of such an attack, or (3) mitigate the effects of circumstances associated with loss of large areas of the facility due to explosions or fires.

Second a definition for *security functions* would indicate those functions necessary to: (1) detect, delay, assess, or respond to an attack against target sets of a nuclear power plant by an adversary possessing the DBT characteristics, (2) mitigate the effects of such an attack; or, (3) mitigate the effects of circumstances associated with loss of large areas of the facility due to explosions or fires. This definition would further state that security functions may be accomplished through security design features or by the operational programs as described in the physical security, training and qualification, and contingency plans (security plans) under 10 CFR 73.55.

Finally, a definition for *security assessment parameters* would indicate: (1) the site characteristics or site parameters where the nuclear power plant or reactor is to, or may, be utilized, which are either postulated in the security assessment or as identified according to 10 CFR 100.21(f), (2) security design features that are outside the scope of the design being addressed at the particular stage of the regulatory process, which are postulated in a security assessment performed under this section; and (3) features of a physical security program under 10 CFR 73.55 which are postulated in a security assessment performed under this section.

Paragraph (b) would specify the objectives of the security assessment process. The security assessment and screening process considers design features within the scope of the

design for which NRC regulatory approval is being sought by the applicant, and programs such as security force, physical protection, emergency operations, safety, maintenance, facility operations, personnel security, and information security relative to the scope of the application. The results of these would ensure that the final design and programs

(1) provide a high level of assurance of the capabilities to detect, delay, assess, respond to, and thwart threats identified in the DBT and

(2) mitigate the effects of circumstances associated with loss of large areas of the site due to explosions or fires.

Paragraph (b)(1) would require the applicant to identify all the target sets. Applicants would list each target set that defines the combination of equipment or operator actions that, if all were prevented from performing their intended safety function or are prevented from being accomplished, would likely result in significant core damage.

Paragraph (b)(2) would require that the security assessment process use a methodology and related tools to evaluate, for each scenario, the effectiveness of candidate security design features in accomplishing security functions. The process of conducting a security assessment includes gathering data that describes the physical and operational aspects of the security design features; assigning values for established probability of detection, assessment, delay, and response; then analyzing the results to determine the effectiveness commensurate with the adversary's capabilities identified in the Commission-approved DBT. The process would also consider the effects that cyber attacks may have upon individual components of each target set grouping. Additionally, the security assessment must consider the effects of the circumstances associated with loss of large areas of the site due to explosions or fires. An assessment methodology can include computer-based tools and simulations, table-top analyses, and analyses by subject matter experts. These analyses would involve the prioritization of targets and the consequences of their loss. During the analysis, the

applicant would (1) identify significant consequences to the facility during the postulated events, (2) for each target set element, determine the result if that target set element were not available or could not perform its intended function,(3) determine the importance of each target set element for each consequence evaluated and, (4) prioritize target set elements for protection for the scenario being considered.

Paragraph (b)(3) would require the security assessment to consider any security assessment parameters identified during previous security assessments (if any). The parameters would include information, within the scope of the design stage being evaluated, related to such things as the topography of the site, security operational program features, and the identification of security design features outside the scope of the design stage being addressed.

Paragraph (b)(4) would require the development and use of a screening process. The screening process would work in conjunction with the evaluation methodology in paragraph (b)(2) as a tool that would determine the practicability of potential security design features. The screening process would have the goal of optimizing the inclusion of security design features in the design phase while considering the impact on safety functions and cost-effectiveness of engineered controls. The methodology used would need to show a clear result by identifying how the assessment objectives were met and how the screening process eliminated security design features from further consideration.

Paragraph (c) would specify the required contents of the security assessment to be performed by the applicant and submitted to the NRC. A complete assessment will include, as required in paragraph (c)(1), a detailed description of the process or methodologies used to develop and identify the target sets. The results of the analysis performed in paragraph (c)(1) would lead to the development of a target set list and related elements. Paragraph (c)(2) would require a target set listing that would include the physical location, identification, description,

size and configuration of the target(s) and related elements.

Paragraph (c)(3) would require that the security assessment include a detailed description of the processes and methodologies used to perform the evaluation, including the screening process for practicability decisions regarding the design features. The applicant would need to describe in detail the assessment methodologies and related tool(s) used to evaluate the candidate design features and provide the version number, date, and basic assumptions used.

Paragraph (c)(4) would require that the security assessment include a listing identifying the security functions for the plant. This would include systems, structures, and components that perform a security function for the stage of the design being evaluated.

Paragraph (c)(5) would require that the security assessment identify the security design features chosen for inclusion into the design and explain how each security design feature provides or enhances the capability of the facility to protect the target sets and related elements against an adversary possessing the DBT characteristics, or to mitigate the effects of circumstances associated with loss of large areas of the facility due to explosions or fires.

Paragraph (c)(6) would require that the applicant include the security assessment parameters used in the assessment (including those identified from the security assessment conducted at the construction permit, standard design approval, design certification, or manufacturing stage, as applicable). Conversely, paragraph (c)(7) would require that the applicant list the security assessment parameters that: (1) were not addressed within the scope of the current design stage and that must be addressed at future design/construction stages as applicable and (2) that are to be incorporated into the development of the security plans required under 10 CFR 73.55.

Paragraphs (d) through (e) would be reserved.

Paragraph (f) would require that each applicant to integrate practicable security design

features into the facility. Under this requirement, the applicant would be obligated, within the scope of the assessment for that given stage in the regulatory process (standard design approval, standard design certification, construction permit, operating license, combined license, and manufacturing license), to incorporate into the nuclear power facility any security design features that were found to be practicable as a result of the security assessment.

Paragraph (g) would require that applicants for an operating license, combined license, and/or manufacturing license ensure that any security design features, found to be practicable as a result of the security assessment and information about the functions they perform, have been integrated into the security plans required by 10 CFR 73.55 and associated appendices.

VIII. Guidance

The NRC is preparing a new regulatory guide that provides examples of acceptable methodologies for developing and submitting a security assessment at the design certification, standard design approval, manufacturing license, construction permit, and operating license phases. In addition, a NUREG report is being prepared to provide guidance on concepts for security protection that might be applied at each phase. Development of the guidance documents is ongoing and final guidance will be published soon after publication of the final rule. The staff is taking steps to keep potential near-term applicants aware of the development of associated implementation guidance, including planned meetings (with cleared individuals) and a pilot effort to evaluate draft implementing guidance. Portions of these guidance documents that contain sensitive information would only be available to those individuals who are authorized and have a need-to-know. However, the NRC believes that access to these portions of the documents is not necessary for stakeholders to provide informed comment on this proposed rule.

IX. 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, 52, 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 § 73.62 is issued under Sections 161b, 161i, of 161o of the AEA, and are not included in 10 CFR 73.81(b). The proposed regulation is subject to criminal penalties because the proposed rule contains substantive requirements.

X. 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 10 CFR. Although an Agreement State may not adopt program elements reserved to the 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, Category "NRC" regulations do not confer regulatory authority on the State.

XI. Availability of Documents

The table below indicates those documents that are available to the public and how they may be obtained. The NRC is making the documents identified below available to interested

persons through one or more of the following methods as indicated.

Public Document Room (PDR). The NRC Public Document Room is located at 11555 Rockville Pike, Rockville, Maryland.

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

NRC's Electronic Reading Room (ERR). The NRC's electronic reading room is located at www.nrc.gov/reading-rm.html.

Document	PDR	Web	ERR
SECY-05-0120, "Security Design Expectations for New Reactor Licensing Activities," (July 6, 2005)	X	X	ML051100233
SRM-SECY-05-0120, "Staff Requirements on SECY-05-0048," (September 9, 2005)	X	X	ML052520334
Environmental Assessment	X	X	ML062300227
Regulatory Analysis	X	X	ML062300184

XII. Plain Language

The Presidential memorandum "Plain Language in Government Writing" published June 10, 1998 (63 FR 31883), directed that the Government's documents be in clear and accessible language. The NRC requests comments on the proposed rule specifically with respect to the clarity and reflectiveness of the language used. Comments should be sent to the address listed under the ADDRESSES caption of this notice.

XIII. Voluntary Consensus Standards

The National Technology Transfer and Advancement Act of 1995, Pub. L. 104-113, requires that Federal agencies use technical standards that are developed or adopted by voluntary consensus standards bodies unless using such a standard is inconsistent with applicable law or is otherwise impractical. The NRC is not aware of any voluntary consensus standard that could be used instead of the proposed Government-unique standards. The NRC will consider using a voluntary consensus standard if an appropriate standard is identified.

XIV. Finding of No Significant Environmental Impact: Availability

The Commission has determined under the National Environmental Policy Act of 1969, as amended, and the Commission's regulations in Subpart A, "National Environmental Policy Act; Regulations Implementing Section 102(2)," of 10 CFR Part 51, "Environmental Protection Regulations for Domestic Licensing and Related Regulatory Functions," that this rule, if adopted, would not be a major Federal action significantly affecting the quality of the human environment and, therefore, an environmental impact statement is not required.

The determination of this environmental assessment is that there will be no significant offsite impact to the public from this action. However, the general public should note that the NRC is seeking public participation and the environmental assessment is available as indicated in Section XI. Comments on any aspect of the environmental assessment may be submitted to the NRC as indicated under the ADDRESSES heading.

The NRC has sent a copy of the environmental assessment and this proposed rule to every State Liaison Officer and requested their comments on the environmental assessment.

XV. Paperwork Reduction Act Statement

The proposed rule contains new or amended information collection requirements that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501, *et seq*). This rule has been submitted to the Office of Management and Budget for review and approval of the information collection requirements.

Type of submission, new or revision:	New.
The title of the information collection	10 CFR Parts 50, 52 and 73; "Security Assessment Requirements for New Nuclear Power Reactors," proposed rule.
The form number if applicable:	N/A.
How often the collection is required:	One time; to be submitted with each application for a design certification, manufacturing license, combined license, construction permit, or operating license.
Who will be required or asked to report:	Designers and manufacturers of commercial nuclear power plants and any person eligible under the Atomic Energy Act to apply for a construction permit, operating license, or combined license for a nuclear power plant.

An estimate of the number of annual responses: 6

The estimated number of annual respondents: 6

An estimate of the total number of hours needed annually to complete the requirement or request: 15,360 hours reporting.

Abstract: The U.S. Nuclear Regulatory Commission is proposing to amend its regulations by adding security assessment requirements for future applicants for a construction permit, operating license, standard design approval, design certification, manufacturing license, or combined license. The proposed amendments would require applicants to assess specific security design features that would be incorporated into the facility and site design to support enhanced security effectiveness. The proposed amendments are needed to ensure that security design features are assessed early in the design and regulatory review process, and not later, when it could be more difficult to incorporate the features. Resolution of security design issues at the early stage of the regulatory review process would result in a more robust security posture requiring less reliance on operational security programs.

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 PDR, 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 Web site at http://www.nrc.gov/public-involve/doc-comment/omb/index.html for 60 days after the signature date of this notice. They are also available at the Rule Forum Web 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 email to INFOCOLLECTS@nrc.gov and to the Desk Officer, John A. Asalone, Office of Information and Regulatory Affairs, NEOB-10202, (**3150-0011, 3150-0151, and 3150-0002 (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.

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.

XVI. Regulatory Analysis

The Commission has prepared a draft regulatory analysis on this proposed regulation. The analysis examines the costs and benefits of the alternatives considered by the Commission. The Commission requests public comments on the draft regulatory analysis. Availability of the regulatory analysis is indicated in Section XI. Comments on the draft analysis may be submitted to the NRC as indicated under the ADDRESSES heading.

XVII. Regulatory Flexibility Certification

In accordance with the Regulatory Flexibility Act (5 U.S.C. 605(b)), the Commission certifies that this rule would not, if promulgated, have a significant economic impact on a substantial number of small entities. This proposed rule affects only the licensing of nuclear power plants. The companies that will apply for an approval, certification, permit, or license in accordance with the regulation affected by this proposed rule do not fall within the scope of the definition of "small entities" set forth in the Regulatory Flexibility Act or the size standards established by the NRC (10 CFR 2.810, “NRC Size Standards”).

XVIII. Backfit Analysis

The NRC has determined that the backfit rule does not apply to this proposed rule and, therefore, a backfit analysis is not required because the proposed rule does not contain any provisions that would impose backfitting as defined in the backfit rule, 10 CFR 50.109, “Backfitting.” The proposed rule would revise the requirements for future standard design certifications, combined licenses, standard design approvals, manufacturing licenses, construction permits, and operating licenses for nuclear power plants. These revisions would not constitute backfits because they are prospective in nature and the backfit rule was not intended to apply to every NRC action that substantially changes the expectations of future applicants. The proposed rule would impose no new requirements on (1) an applicant filing for a permit or license before the effective date of the final rule, (2) a design certification rule in Appendices A through D of 10 CFR Part 52, or (3) the current fleet of operating nuclear power reactors.

List of Subjects

10 CFR Part 50

Antitrust, Classified information, Criminal penalties, Fire protection, Intergovernmental relations, Nuclear power plants and reactors, Radiation protection, Reactor siting criteria, Reporting and recordkeeping requirements.

10 CFR Part 52

Administrative practice and procedure, Antitrust, Backfitting, Combined license, Early site permit, Emergency planning, Fees, Inspection, Limited work authorization, Nuclear power plants and reactors, Probabilistic risk assessment, Prototype, Reactor siting criteria, Redress of

site, Reporting and recordkeeping requirements, Standard design, Standard design certification.

10 CFR Part 73

Criminal penalties, Export, Hazardous materials transportation, Import, Nuclear materials, Nuclear power plants and reactors, Reporting and recordkeeping requirements, Security measures.

For the reasons set out in the preamble and under the authority of the Atomic Energy Act of 1954, as amended; the Energy Reorganization Act of 1974, as amended; and 5 U.S.C. 553, the NRC is proposing to adopt the following amendments to 10 CFR Parts 50, 52, and 73.

PART 50—DOMESTIC LICENSING OF PRODUCTION AND UTILIZATION FACILITIES

1. The authority citation for Part 50 continues to read as follows:

AUTHORITY: Secs. 102, 103, 104, 105, 161, 182, 183, 186, 189, 68 Stat. 936, 937, 938, 948, 953, 954, 955, 956, as amended, sec. 234, 83 Stat. 444, as amended (42 U.S.C. 2132, 2133, 2134, 2135, 2201, 2232, 2233, 2236, 2239, 2282); secs. 201, as amended, 202, 206, 88 Stat. 1242, as amended, 1244, 1246 (42 U.S.C. 5841, 5842, 5846); sec. 1704, 112 Stat. 2750 (44 U.S.C. 3504 note). Section 50.7 also issued under Pub. L. 95-601, sec. 10, 92 Stat. 2951 (42 U.S.C. 5841). Section 50.10 also issued under secs. 101, 185, 68 Stat. 955, as amended (42 U.S.C. 2131, 2235); sec. 102, Pub. L. 91-190, 83 Stat. 853 (42 U.S.C. 4332). Sections 50.13, 50.54(dd), and 50.103 also issued under sec. 108, 68 Stat. 939, as amended (42 U.S.C. 2138). Sections 50.23, 50.35, 50.55, and 50.56 also issued under sec. 185, 68 Stat. 955 (42 U.S.C. 2235). Sections 50.33a, 50.55a and Appendix Q also issued under sec. 102,

Pub. L. 91-190, 83 Stat. 853 (42 U.S.C. 4332). Sections 50.34 and 50.54 also issued under sec. 204, 88 Stat. 1245 (42 U.S.C. 5844). Sections 50.58, 50.91, and 50.92 also issued under Pub. L. 97-415, 96 Stat. 2073 (42 U.S.C. 2239). Section 50.78 also issued under sec. 122, 68 Stat. 939 (42 U.S.C. 2152). Sections 50.80 and 50.81 also issued under sec. 184, 68 Stat. 954, as amended (42 U.S.C. 2234). Appendix F also issued under sec. 187, 68 Stat. 955 (42 U.S.C. 2237).

2. In § 50.34, paragraph (h) is redesignated as paragraph (m) and revised, paragraphs (i) through (l) are reserved, and a new paragraph (h) is added to read as follows:

§ 50.34 Contents of applications; technical information.

* * * * *

(h) *Security assessment for design*.

(1) *Construction permit application*. Each application for a construction permit filed after [THE EFFECTIVE DATE OF FINAL RULE] must describe how the applicant will comply with 10 CFR 73.62 in completing the design of the nuclear power plant, including a description of the applicant's plan for conducting a security assessment which complies with § 73.62(d) of this chapter, and describes the security design features incorporated into the final design of the site.

(2) *Operating license application*. Each application for an operating license filed after [AFTER THE EFFECTIVE DATE OF FINAL RULE] must contain a security assessment which complies with the requirements of 10 CFR 73.62.

(i) - (l) [Reserved]

(m) Conformance with the Standard Review Plan (SRP).

(1)(i) Applications for light water cooled nuclear power plant operating licenses

docketed after May 17, 1982, must include an evaluation of the facility against the SRP in effect on May 17, 1982, or the SRP revision in effect 6 months before the docket date of the application, whichever is later.

(ii) Applications for light water cooled nuclear power plant construction permits, manufacturing licenses, and preliminary or final design approvals for standard plants docketed after May 17, 1982, must include an evaluation of the facility against the SRP in effect on May 17, 1982, or the SRP revision in effect 6 months before the docket date of the application, whichever is later.

(2) The evaluation required by this section must include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for a facility and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where a difference exists, the evaluation must discuss how the alternative proposed provides an acceptable method of complying with those rules or regulations of Commission, or portions thereof, that underlie the corresponding SRP acceptance criteria.

(3) The SRP was issued to establish criteria that the NRC staff intends to use in evaluating whether an applicant/licensee meets the Commission's regulations. The SRP is not a substitute for the regulations, and compliance is not a requirement. Applicants shall identify differences from the SRP acceptance criteria and evaluate how the proposed alternatives to the SRP criteria provide an acceptable method of complying with the Commission's regulations.

3. In Appendix M to Part 50, paragraph 4(c) is added to read as follows:

Appendix M to 10 CFR Part 50—Standardization of Design: Manufacture of Nuclear Power Reactors: Construction and Operation of Nuclear Power Reactors Manufactured pursuant to Commission License.

* * * * *

4 * * *

(c) Each application for a manufacturing license filed after [THE EFFECTIVE DATE OF FINAL RULE] must describe how the applicant will comply with 10 CFR 73.62 of this chapter in completing the design of the nuclear power plant, including a description of the applicant's plan for conducting a security assessment that complies with § 73.62(d) of this chapter, and describes the security design features incorporated into the final design of the facility.

* * * * *

4. In Appendix O to Part 50, paragraph 3 is revised to read as follows:

Appendix O to 10 CFR Part 50—Standardization of Design: Staff Review of Standard Designs.

* * * * *

3. The submittal for review of the standard design must include the information described in §§ 50.33 (a) through (d) and the applicable technical information required by §§ 50.34 (a), (b) and (h), as appropriate, and § 50.34a (other than that required by §§ 50.34(a)(6) and (10), 50.34(b)(1), (6)(i), (ii), (iv), and (v) and 50.34(b) (7) and (8)). The submittal must also include a description, analysis and evaluation of the interfaces between the submitted design and the balance of the nuclear power plant. With respect to the requirements of § 50.34(a)(1), the submittal for review of a standard design must include the site parameters postulated for the design, and an analysis and evaluation of the design in terms of such postulated site parameters. The information submitted under § 50.34(a)(7) must be limited to the quality assurance program to be applied to the design, procurement, and fabrication of the structures, systems, and components for which design review has been requested and the information submitted under § 50.34(a)(9) must be limited to the qualifications of the person

submitting the standard design to design the reactor or major portion thereof. The submittal must also include information pertaining to design features that affect plans for coping with emergencies in the operation of the reactor or major portion thereof.

* * * * *

PART 52—EARLY SITE PERMITS; STANDARD DESIGN CERTIFICATIONS; AND COMBINED LICENSES FOR NUCLEAR POWER PLANTS

5. The authority citation for Part 52 continues to read as follows:

AUTHORITY: Secs. 103, 104, 161, 182, 183, 186, 189, 68 Stat. 936, 948, 953, 954, 955, 956, as amended, sec. 234, 83 Stat. 444, as amended (42 U.S.C. 2133, 2201, 2232, 2233, 2236, 2239, 2282); secs. 201, 202, 206, 88 Stat. 1242, 1244, 1246, as amended (42U.S.C. 5841, 5842, 5846); sec. 1704, 112 Stat. 2750 (44 U.S.C. 3504 note).

6. In § 52.3, paragraph (e) is revised to read as follows:

§ 52.3 Definitions.

* * * * *

(e) All other terms in this part have the meaning set out in 10 CFR 50.2, 10 CFR 73.2, 10 CFR 73.62, or section 11 of the Atomic Energy Act, as applicable.

7. In § 52.47, paragraphs (c) through (f) are reserved, and a new paragraph (g) is added to read as follows:

§ 52.47 Contents of applications.

* * * * *

(c)–(f) [Reserved]

(g) *Security assessment for design*. Each application for a standard design certification filed after [EFFECTIVE DATE OF FINAL RULE] must contain a security assessment that complies with the requirements of 10 CFR 73.62 of this chapter and describe the security design features incorporated into the standard design certification.

8. Section 52.54 is revised to read as follows:

§ 52.54 Issuance of standard design certification.

(a) The Commission shall issue a standard design certification in the form of a rule for the design that is the subject of the application after–

(1) Conducting a rulemaking proceeding under § 52.51 on an application for a standard design certification;

(2) Receiving the report to be submitted by the Advisory Committee on Reactor Safeguards under § 52.53; and

(3) Determining that the application meets the applicable standards and requirements of the Atomic Energy Act and the Commission's regulations.

(b) The design certification rule must specify the site parameters, security design features, security assessment parameters, and any additional requirements of the design certification rule.

9. In § 52.79, paragraphs (e) through (f) are reserved, and a new paragraph (g) is added to read as follows:

§ 52.79 Contents of applications; technical information.

* * * * *

(e)–(f) [Reserved]

(g) *Security Assessment for Design*. Each application for a combined license filed after [EFFECTIVE DATE OF FINAL RULE] must contain a security assessment that complies with the requirements of 10 CFR 73.62 of this chapter, and describe the security design features incorporated into the design of the nuclear power plant.

(1) If the application references either a standard design certification rule under subpart B of this part adopted after [EFFECTIVE DATE OF FINAL RULE], or the use of a nuclear power reactor manufactured under a manufacturing license in appendix M to this part issued after [EFFECTIVE DATE OF FINAL RULE], then—

(i) The security assessment performed for the design certification or manufacturing license must be incorporated by reference into the combined license application,

(ii) The security assessment for the combined license application need not address the design of the plant within the scope of the design certification or manufacturing license,

(iii) The security assessment for the combined license must identify the security functions, security design features and security operational programs, and describe how security functions, not previously evaluated at the design stage, are addressed.

(2) If the application references a standard design certification rule in appendices A through D of this part, then—

(i) The security assessment for the combined license application need not address the design of the plant within the scope of the design certification,

(ii) The security assessment for the combined license must identify the security functions, security design features and security operational programs, and describe how security functions, not previously evaluated at the design certification stage, are addressed.

(3) If the application is filed no later than [INSERT DATE 6 MONTHS AFTER EFFECTIVE DATE OF FINAL RULE], the security assessment and any associated design changes may be filed no later than [INSERT DATE 12 MONTHS AFTER EFFECTIVE DATE OF FINAL RULE]. A filed application, which the NRC determines is complete except for the lack of the security assessment, will be considered complete and acceptable for docketing under 10 CFR 2.101.

10. In Appendix M to Part 52, paragraph 4(c) is added to read as follows:

Appendix M to 10 CFR Part 52—Standardization of Design: Manufacture of Nuclear Power Reactors: Construction and Operation of Nuclear Power Reactors Manufactured Pursuant to Commission License.

* * * * *

4 * * *

(c) Each application for a manufacturing license filed after [THE EFFECTIVE DATE OF FINAL RULE] must describe how the applicant will comply with 10 CFR 73.62 of this chapter in completing the design of the nuclear power plant, including a description of the applicant's plan for conducting a security assessment that complies with § 73.62(d) of this chapter, and describe the security design features incorporated into the final design of the facility.

* * * * *

11. In Appendix O to Part 52, paragraph 3 is revised to read as follows:

Appendix O to 10 CFR Part 52—Standardization of Design: Staff Review of Standard Designs.

* * * * *

3. The submittal for review of the standard design must include the information described in §§ 50.33 (a) through (d) of this chapter and the applicable technical information required by §§ 50.34 (a), (b), and (h), as appropriate, and 50.34a of this chapter (other than that required by §§ 50.34(a) (6) and (10), 50.34(b)(1), (6) (i), (ii), (iv), and (v) and 50.34(b) (7) and (8) of this chapter). The submittal must also include a description, analysis and evaluation of the interfaces between the submitted design and the balance of the nuclear power plant. With respect to the requirements of § 50.34(a)(1) of this chapter, the submittal for review of a standard design must include the site parameters postulated for the design, and an analysis and evaluation of the design in terms of such postulated site parameters. The information submitted under § 50.34(a)(7) of this chapter must be limited to the quality assurance program to be applied to the design, procurement, and fabrication of the structures, systems, and components for which design review has been requested and the information submitted under § 50.34(a)(9) of this chapter must be limited to the qualifications of the person submitting the standard design to design the reactor or major portion thereof. The submittal must also include information pertaining to design features that affect plans for coping with emergencies in the operation of the reactor or major portion thereof.

* * * * *

PART 73—PHYSICAL PROTECTION OF PLANTS AND MATERIALS

12. The authority citation for Part 73 continues to read as follows:

AUTHORITY: Secs. 53, 161, 68 Stat. 930, 948, as amended, sec. 147, 94 Stat. 780 (42 U.S.C. 2073, 2167, 2201); sec. 201, as amended, 204, 88 Stat. 1242, as amended, 1245, sec. 1701, 106 Stat. 2951, 2952, 2953 (42 U.S.C. 5841, 5844, 2297f); sec. 1704, 112 Stat. 2750 (44

U.S.C. 3504 note).Section 73.1 also issued under secs. 135, 141, Pub. L. 97-425, 96 Stat. 2232, 2241 (42 U.S.C, 10155, 10161). Section 73.37(f) also issued under sec. 301, Pub. L. 96-295, 94 Stat. 789 (42 U.S.C. 5841 note). Section 73.57 is issued under sec. 606, Pub. L. 99-399, 100 Stat. 876 (42 U.S.C. 2169).

13. In § 73.8, paragraph (b) is revised to read as follows:

§ 73.8 Information collection requirements: OMB approval.

* * * * *

(b) The approved information collection requirements contained in this part appear in §§ 73.5, 73.18, 73.19, 73.20, 73.21, 73.24, 73.25, 73.26, 73.27, 73.37, 73.40, 73.45, 73.46, 73.50, 73.55, 73.56, 73.57, 73.58, 73.60, 73.62, 73.67, 73.70, 73.71, 73.72, 73.73, 73.74, and appendices B, C, and G.

14. Section 73.55 is revised to read as follows:

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

(a) Introduction.

(1) By **[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 Commission for review and approval.

(2) The amended security plans must be submitted as specified in § 50.4 of this chapter and must describe how the revised requirements of this section will be implemented by the licensee, to include a proposed implementation schedule.

(3) The licensee shall implement the existing approved security plans and associated Commission orders until Commission approval of the amended security plans, unless otherwise authorized by the Commission.

(4) The licensee is responsible 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.

(5) Applicants for an operating license under the provisions of part 50 of this chapter, or holders of a combined license under the provisions of part 52 of this chapter, shall satisfy the requirements of this section before the receipt of special nuclear material in the form of fuel assemblies.

(6) For licenses issued after [EFFECTIVE DATE OF THE FINAL RULE], licensees shall design construct, and equip the central alarm station and secondary alarm station to equivalent standards.

(i) Licensees shall apply the requirements for the central alarm station listed in paragraphs (e)(6)(v), (e)(7)(iii), and (i)(8)(ii) of this section to the secondary alarm station as well as the central alarm station.

(ii) Licensees shall comply with the requirements of paragraph (i)(4) of this section such that both alarm stations are provided with equivalent capabilities for detection, assessment, monitoring, observation, surveillance, and communications.

(7) For license applications filed after [EFFECTIVE DATE OF THE FINAL RULE], the security plans, as required by § 73.55 and associated Appendices, must include security design features identified in accordance with § 73.62.

(b) General performance objective and requirements.

(1) The licensee shall establish and maintain a physical protection program, to include a security organization which will have as its objective to 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 health and safety.

(2) The physical protection program must be designed to detect, assess, intercept, challenge, delay, and neutralize threats up to and including the design basis threat of radiological sabotage as stated in § 73.1(a), at all times.

(3) The licensee physical protection program must be designed and implemented to satisfy the requirements of this section and ensure that no single act, as bounded by the design basis threat, can disable the personnel, equipment, or systems necessary to prevent significant core damage and spent fuel sabotage.

(4) The physical protection program must include diverse and redundant equipment, systems, technology, programs, supporting processes, and implementing procedures.

(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 the physical protection program, including the ability of armed and unarmed personnel to perform assigned duties and responsibilities required by the approved security plans and licensee procedures.

(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 to protect target sets described in paragraph (f) of this section and appendix C to this part, through implementation of the licensee protective strategy.

(7) The licensee shall establish, maintain, and follow an access authorization program

in accordance with § 73.56.

(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, implement, and maintain 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.

(8) The licensee shall ensure that its corrective action program assures that failures, malfunctions, deficiencies, deviations, defective equipment and nonconformances in security program components, functions, or personnel are promptly identified and corrected. Measures shall ensure that the cause of any of these conditions is determined and that corrective action is taken to preclude repetition.

(c) Security plans.

(1) Licensee security plans. Licensee security plans must implement Commission requirements and must describe:

(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

(ii) Site-specific conditions that affect implementation of Commission requirements.

(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.

(3) Physical security plan.

(i) The licensee shall establish, maintain, and implement a Commission-approved physical security plan that describes how the performance objective and requirements set forth in this section will be implemented.

(ii) The physical security plan must describe the facility location and layout, the security organization and structure, duties and responsibilities of personnel, defense-in-depth implementation that describes components, equipment and technology used.

(4) Training and qualification plan.

(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.

(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.

(5) Safeguards contingency plan.

(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.

(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.

(6) Implementing procedures.

(i) The licensee shall establish, maintain, and implement written procedures that

document the structure of the security organization, detail the specific duties and responsibilities of each position, and implement Commission requirements through the approved security plans.

(ii) Implementing procedures need not be submitted to the Commission for prior approval, but are subject to inspection by the Commission.

(iii) Implementing procedures must detail the specific actions to be taken and decisions to be made by each position of the security organization to implement the approved security plans.

(iv) The licensee shall:

(A) Develop, maintain, enforce, review, and revise security implementing procedures.

(B) Provide a process for the written approval of implementing procedures and revisions by the individual with overall responsibility for the security functions.

(C) Ensure that changes made to implementing procedures do not decrease the effectiveness of any procedure to implement and satisfy Commission requirements.

(7) Plan revisions. The licensee shall revise approved security plans as necessary to ensure the effective implementation of Commission regulations and the licensee's protective strategy. Commission approval of revisions made pursuant to this paragraph is not required, provided that revisions meet the requirements of § 50.54(p) of this chapter. Changes that are beyond the scope allowed per § 50.54(p) of this chapter shall be submitted as required by §§ 50.90 of this chapter or § 73.5.

(d) Security organization.

(1) The licensee shall establish and maintain a security organization designed, staffed, trained, and equipped to provide early detection, assessment, and response to unauthorized activities within any area of the facility.

(2) The security organization must include:

(i) A management system that provides oversight of the onsite physical protection program.

(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.

(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 part 73 and the Commission-approved training and qualification plan.

(4) The licensee may not assign an individual to any position involving detection, assessment, or response to unauthorized activities unless that individual has satisfied the requirements of § 73.56.

(5) If a contracted security force is used to implement the onsite physical protection program, the licensee's written agreement with the contractor must be retained by the licensee as a record for the duration of the contract and must clearly state the following conditions:

(i) The licensee is responsible to the Commission for maintaining the physical protection program in accordance with Commission orders, Commission regulations, and the approved security plans.

(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.

(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.

(iv) An individual 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 to part 73 and the Commission-approved training and qualification plan.

(v) Upon the request of an authorized representative of the Commission, the contractor security employees shall demonstrate the ability to perform their assigned duties and responsibilities effectively.

(vi) Any license for possession and ownership of enhanced weapons will reside with the licensee.

(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.

(1) The licensee shall describe in the approved security plans, the design, construction, and function of physical barriers and barrier systems used and shall ensure that each barrier and barrier system is designed and constructed to satisfy the stated function of the barrier and barrier system.

(2) The licensee shall retain in accordance with § 73.70, all analyses, comparisons, and descriptions of the physical barriers and barrier systems used to satisfy the requirements of this section, and shall protect these records as safeguards information in accordance with the requirements of § 73.21.

(3) Physical barriers must:

(i) Clearly delineate the boundaries of the area(s) for which the physical barrier provides

protection or a function, such as protected and vital area boundaries and stand-off distance.

(ii) Be designed and constructed to protect against the design basis threat commensurate to the required function of each barrier and in support of the licensee protective strategy.

(iii) Provide visual deterrence, delay, and support access control measures.

(iv) Support effective implementation of the licensee's protective strategy.

(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.

(5) Isolation zone.

(i) An isolation zone must be maintained in outdoor areas adjacent to the protected area perimeter barrier. The isolation zone shall be:

(A) Designed and of sufficient size to permit unobstructed observation and assessment of activities on either side of the protected area barrier.

(B) Equipped with intrusion detection equipment capable of detecting both attempted and actual penetration of the protected area perimeter barrier and assessment equipment 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.

(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.

(v) The reactor control room, the central alarm station, and the location within which the last access control function for access to the protected area is performed, must be bullet-resisting.

(vi) All exterior areas within the protected area must be periodically checked to detect and deter unauthorized activities, personnel, vehicles, and materials.

(7) Vital areas.

(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)(3) of this section.

(ii) More than one vital area may be located within a single protected area.

(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 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) of this section.

(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.

(iv) Deter, detect, delay, or prevent vehicle use as a means of transporting unauthorized personnel or materials to gain unauthorized access beyond a vehicle barrier system, gain proximity to a protected area or vital area, or otherwise penetrate the protected area perimeter.

(v) Periodically check the operation of active vehicle barriers and provide a secondary power source or a means of mechanical or manual operation, in the event of a power failure to

ensure that the active barrier can be placed in the denial position within the time line required to prevent unauthorized vehicle access beyond the required standoff distance.

(vi) Provide surveillance and observation of vehicle barriers and barrier systems to detect unauthorized activities and to ensure the integrity of each vehicle barrier and barrier system.

(9) Waterways.

(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) of this section.

(ii) The licensee shall delineate areas from which a waterborne vehicle must be restricted and install waterborne vehicle control measures, where applicable.

(iii) The licensee shall monitor waterway approaches and adjacent areas to ensure early detection, assessment, and response to unauthorized activity or proximity, and to ensure the integrity of installed waterborne vehicle control measures.

(iv) Where necessary to meet the requirements of this section, licensees shall coordinate with local, state, and Federal agencies having jurisdiction over waterway approaches.

(10) Unattended openings in any barrier established to meet the requirements of this section that are 620 cm^2 (96.1 in^2) or greater in total area and have a smallest dimension of 15 m (5.9 in) or greater, must be secured and monitored at a frequency that would prevent exploitation of the opening consistent with the intended function of each barrier.

(f) Target sets.

(1) The licensee shall document in site procedures the process used to develop and identify target sets, to include analyses and methodologies used to determine and group the

target set equipment or elements.

(2) The licensee shall consider the effects that cyber attacks may have upon individual equipment or elements of each target set or grouping.

(3) Target set equipment or elements that are not contained within a protected or vital area must be explicitly identified in the approved security plans and protective measures for such equipment or elements must be addressed by the licensee's protective strategy in accordance with appendix C to this part.

(4) The licensee shall implement a program for the oversight of plant equipment and systems documented as part of the licensee protective strategy to ensure that changes to the configuration of the identified equipment and systems do not compromise the licensee's capability to prevent significant core damage and spent fuel sabotage.

(g) Access control.

(1) The licensee shall:

(i) Control all points of personnel, vehicle, and material access into any area, or beyond any physical barrier or barrier system, established to meet the requirements of this section.

(ii) Control all points of personnel and vehicle access into vital areas in accordance with access authorization lists.

(iii) During non-emergency conditions, limit unescorted access to the protected area and vital areas to only those individuals who require unescorted access to perform assigned duties and responsibilities.

(iv) Monitor and ensure the integrity of access control systems.

(v) Provide supervision and control over the badging process to prevent unauthorized bypass of access control equipment located at or outside of the protected area.

(vi) Isolate the individual responsible for the last access control function (controlling admission to the protected area) within a bullet-resisting structure to assure the ability to

respond or to summon assistance in response to unauthorized activities.

(vii) In response to specific threat and security 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.

(2) In accordance with the approved security plans and before granting unescorted access through an access control point, the licensee shall:

(i) Confirm the identity of individuals.

(ii) Verify the authorization for access of individuals, vehicles, and materials.

(iii) Search individuals, vehicles, packages, deliveries, and materials in accordance with paragraph (h) of this section.

(iv) Confirm, in accordance with industry shared lists and databases, that individuals have not been denied access to another power reactor facility.

(3) Access control points must be:

(i) Equipped with locking devices, intrusion detection equipment, and monitoring, observation, and surveillance equipment, as appropriate.

(ii) Located outside or concurrent with, the physical barrier system through which it controls access.

(4) Emergency conditions.

(i) The licensee shall design the access control system to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions.

(ii) Under emergency conditions, the licensee shall implement procedures to ensure that:

(A) Authorized emergency personnel are provided prompt access to affected areas and

equipment.

(B) Attempted or actual unauthorized entry to vital equipment is detected.

(C) The capability to prevent significant core damage and spent fuel sabotage is maintained.

(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.

(5) Vehicles.

(i) The licensee shall exercise control over all vehicles while inside the protected area and vital areas to ensure they are used only by authorized persons and for authorized purposes.

(ii) Vehicles inside the protected area or vital areas must be operated by an individual authorized unescorted access to the area, or must be escorted by an individual trained, qualified, and equipped to perform vehicle escort duties, while inside the area.

(iii) Vehicles inside the protected area must be limited to plant functions or emergencies, and must be disabled when not in use.

(iv) Vehicles transporting hazardous materials inside the protected area must be escorted by an armed member of the security organization.

(6) Access control devices.

(i) Identification badges. The licensee shall implement a numbered photo identification badge/key-card system for all individuals authorized unescorted access to the protected area and vital areas.

(A) Identification badges may be removed from the protected area only when measures are in place to confirm the true identity and authorization for unescorted access of the badge holder before allowing unescorted access to the protected area.

(B) Except where operational safety concerns require otherwise, identification badges must be clearly displayed by all individuals while inside the protected area and vital areas.

(C) The licensee shall maintain a record, to include the name and areas to which unescorted access is granted, of all individuals to whom photo identification badge/key-cards have been issued.

(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:

(A) Issue access control devices only to individuals who require unescorted access to perform official duties and responsibilities.

(B) Maintain a record, to include name and affiliation, of all individuals to whom access control devices have been issued, and implement a process to account for access control devices at least annually.

(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 a recognized identification card issued by a local, state, or Federal Government agency that includes a photo or contains physical characteristics of the individual requesting escorted access.

(C) Maintain a visitor control register in which all visitors shall register their name, date, time, purpose of visit, employment affiliation, citizenship, and name of the individual to be visited before being escorted into any protected or vital area.

(D) Issue a visitor badge to all visitors that clearly indicates that an escort is required.

(E) Escort all visitors, at all times, while inside the protected area and vital areas.

(ii) Individuals not employed by the licensee but who require frequent and extended unescorted access to the protected area and vital areas shall satisfy the access authorization requirements of § 73.56 and part 26 of this chapter and shall be issued a non-employee photo identification badge that is easily distinguished from other identification badges before being allowed unescorted access to the protected area. Non-employee photo identification badges must indicate:

(A) Non-employee, no escort required.

(B) Areas to which access is authorized.

(C) The period for which access is authorized.

(D) The individual's employer.

(E) A means to determine the individual's emergency plan assembly area.

(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.

(i) Escorts shall be authorized unescorted access to all areas in which they will perform

escort duties.

(ii) Individuals assigned to escort visitors shall be provided a means of timely communication with both alarm stations in a manner that ensures the ability to summon assistance when needed.

(iii) Individuals assigned to vehicle escort duties shall be provided a means of continuous communication with both alarm stations to ensure the ability to summon assistance when needed.

(iv) Escorts shall be knowledgeable of those activities that are authorized to be performed within the areas for which they are assigned to perform escort duties and must also be knowledgeable of those activities that are authorized to be performed by any individual for which the escort is assigned responsibility.

(v) Visitor to escort ratios shall be limited to 10 to 1 in the protected area and 5 to 1 in vital areas, provided that the necessary observation and control requirements of this section can be maintained by the assigned escort over all visitor activities.

(h) Search programs.

(1) At each designated access control point into the owner controlled area and protected area, the licensee shall search individuals, vehicles, packages, deliveries, and materials in accordance with the requirements of this section and the approved security plans, before granting access.

(i) The objective of the search program must be to deter, detect, and prevent the introduction of unauthorized firearms, explosives, incendiary devices, or other unauthorized materials and devices into designated areas in which the unauthorized items could be used to disable personnel, equipment, and systems necessary to meet the performance objective and requirements of paragraph (b) of this section.

(ii) The search requirements for unauthorized firearms, explosives, incendiary devices,

or other unauthorized materials and devices must be accomplished through the use of equipment capable of detecting these unauthorized items and through visual and hands-on physical searches, as needed to ensure all items are identified before granting access.

(iii) Only trained and qualified members of the security organization, and other trained and qualified personnel designated by the licensee, shall perform search activities or be assigned duties and responsibilities required to satisfy observation requirements for the search activities.

(2) The licensee shall establish and implement written search procedures for all access control points before granting access to any individual, vehicle, package, delivery, or material.

(i) Search procedures must ensure that items possessed by an individual, or contained within a vehicle or package, must be clearly identified as not being a prohibited item before granting access beyond the access control point for which the search is conducted.

(ii) The licensee shall visually and physically hand search all individuals, vehicles, and packages containing items that cannot be or are not clearly identified by search equipment.

(3) Whenever search equipment is out of service or is not operating satisfactorily, trained and qualified members of the security organization shall conduct a hands-on physical search of all individuals, vehicles, packages, deliveries, and materials that would otherwise have been subject to equipment searches.

(4) When an attempt to introduce unauthorized items has occurred or is suspected, the licensee shall implement actions to ensure that the suspect individuals, vehicles, packages, deliveries, and materials are denied access and shall perform a visual and hands-on physical search to determine the absence or existence of a threat.

(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.

(6) Vehicle areas to be searched must include, but are not limited to, the cab, engine compartment, undercarriage, and cargo area.

(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 submitted to the Commission for prior review and approval and must be identified in the approved security plans.

(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 least one of which must be protected in accordance with the requirements of paragraphs (e)(6)(v), (e)(7)(iii), and (i)(8)(ii) of this section.

(3) The licensee’s intrusion detection system must be designed to ensure that both alarm station operators:

(i) Are concurrently notified of the alarm annunciation.

(ii) Are capable of making a timely assessment of the cause of each alarm annunciation.

(iii) Possess the capability to initiate a timely response in accordance with the approved security plans, licensee protective strategy, and implementing procedures.

(4) Both alarm stations must be equipped with equivalent capabilities for detection and communication, and must be equipped with functionally equivalent assessment, monitoring, observation, and surveillance capabilities to support the effective implementation of the approved security plans and the licensee protective strategy in the event that either alarm station is disabled.

(i) The licensee shall ensure that a single act cannot remove the capability of both alarm stations to detect and assess unauthorized activities, respond to an alarm, summon offsite assistance, implement the protective strategy, provide command and control, or otherwise prevent significant core damage and spent fuel sabotage.

(ii) The alarm station functions in paragraph (i)(4) of this section must remain operable from an uninterruptible backup power supply in the event of the loss of normal power.

(5) Detection. Detection capabilities must be provided by security organization personnel and intrusion detection equipment, and shall be defined in implementing procedures. Intrusion detection equipment must be capable of operating as intended under the conditions encountered at the facility.

(6) Assessment. Assessment capabilities must be provided by security organization personnel and video assessment equipment, and shall be described in implementing procedures. Video assessment equipment must be capable of operating as intended under the conditions encountered at the facility and must provide video images from which accurate and timely assessments can be made in response to an alarm annunciation or other notification of unauthorized activity.

(7) The licensee intrusion detection and assessment system must:

(i) Ensure that the duties and responsibilities assigned to personnel, the use of equipment, and the implementation of procedures provides the detection and assessment capabilities necessary to meet the requirements of paragraph (b) of this section.

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

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

(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.

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

(vi) Maintain a record of all alarm annunciations, the cause of each alarm, and the disposition of each alarm.

(8) Alarm stations.

(i) Both alarm stations must be continuously staffed by at least one trained and qualified member of the security organization.

(ii) The interior of the central alarm station must not be visible from the perimeter of the protected area.

(iii) The licensee may not permit any activities to be performed within either alarm station that would interfere with an alarm station operator’s ability to effectively execute assigned detection, assessment, surveillance, and communication duties and responsibilities.

(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.

(v) The licensee's 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.

(9) Surveillance, observation, and monitoring.

(i) The physical protection program must include the capability for surveillance, observation, and monitoring in a manner that provides early detection and assessment of unauthorized activities.

(ii) The licensee shall provide continual surveillance, observation, and monitoring of all areas identified in the approved security plans as requiring surveillance, observation, and monitoring to ensure early detection of unauthorized activities and to ensure the integrity of physical barriers or other components of the physical protection program.

(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.

(B) Surveillance, observation, and monitoring requirements may be accomplished by direct observation or video technology.

(iii) The licensee shall provide random patrols of all accessible areas containing target set equipment.

(A) Armed security patrols shall periodically check designated areas and shall inspect vital area entrances, portals, and external barriers.

(B) Physical barriers must be inspected at random intervals to identify tampering and degradation.

(C) Security personnel shall be trained to recognize indications of tampering as

necessary to perform assigned duties and responsibilities as they relate to safety and security systems and equipment.

(iv) Unattended openings that are not monitored by intrusion detection equipment must be observed by security personnel at a frequency that would prevent exploitation of that opening.

(v) Upon detection of unauthorized activities, tampering, or other threats, the licensee shall initiate actions consistent with the approved security plans, the licensee protective strategy, and implementing procedures.

(10) Video technology.

(i) The licensee shall maintain in operable condition all video technology used to satisfy the monitoring, observation, surveillance, and assessment requirements of this section.

(ii) Video technology must be:

(A) Displayed concurrently at both alarm stations.

(B) Designed to provide concurrent observation, monitoring, and surveillance of designated areas from which an alarm annunciation or a notification of unauthorized activity is received.

(C) Capable of providing a timely visual display from which positive recognition and assessment of the detected activity can be made and a timely response initiated.

(D) Used to supplement and limit the exposure of security personnel to possible attack.

(iii) The licensee shall implement controls for personnel assigned to monitor video technology to ensure that assigned personnel maintain the level of alertness required to effectively perform the assigned duties and responsibilities.

(11) Illumination.

(i) The licensee shall ensure that all areas of the facility, to include appropriate portions of the owner controlled area, are provided with illumination necessary to satisfy the

requirements of this section.

(ii) The licensee shall provide a minimum illumination level of 0.2 footcandle measured horizontally at ground level, in the isolation zones and all exterior areas within the protected area, or may augment the facility illumination system, to include patrols, responders, and video technology, with low-light technology capable of meeting the detection, assessment, surveillance, observation, monitoring, and response requirements of this section.

(iii) The licensee shall describe in the approved security plans how the lighting requirements of this section are met and, if used, the type(s) and application of low-light technology used.

(j) Communication requirements.

(1) The licensee shall establish and maintain, continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations.

(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.

(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.

(4) The following continuous communication capabilities must terminate in both alarm stations required by this section:

(i) Conventional telephone service.

(ii) Radio or microwave transmitted two-way voice communication, either directly or through an intermediary.

(iii) A system for communication with all control rooms, on-duty operations personnel,

escorts, local, state, and Federal law enforcement agencies, and all other personnel necessary to coordinate both onsite and offsite responses.

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

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

(k) Response requirements.

(1) Personnel and equipment.

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

(ii) The licensee shall provide and maintain firearms, ammunition, and equipment capable of performing functions commensurate to the needs of each armed member of the security organization to carry out their assigned duties and responsibilities in accordance with the approved security plans, the licensee protective strategy, implementing procedures, and the site specific conditions under which the firearms, ammunition, and equipment will be used.

(iii) The licensee shall describe in the approved security plans, all firearms and equipment to be possessed by and readily available to, armed personnel to implement the protective strategy and carry out all assigned duties and responsibilities. This description must include the general distribution and assignment of firearms, ammunition, body armor, and other equipment used.

(iv) The licensee shall ensure that all firearms, ammunition, and equipment required by the protective strategy are in sufficient supply, are in working condition, and are readily

available for use in accordance with the licensee protective strategy and predetermined time lines.

(v) The licensee shall ensure that all armed members of the security organization are trained in the proper use and maintenance of assigned weapons and equipment in accordance with appendix B to part 73.

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

(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.

(i) Armed responders.

(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.

(B) Armed responders shall be available at all times inside the protected area and may not be assigned any other duties or responsibilities that could interfere with assigned response duties.

(ii) Armed security officers.

(A) Armed security officers designated to strengthen response capabilities shall be onsite and available at all times to carry out assigned response duties.

(B) The minimum number of armed security officers must be documented in the approved security plans.

(iii) The licensee shall ensure that training and qualification requirements accurately reflect the duties and responsibilities to be performed.

(iv) The licensee shall ensure that all firearms, ammunition, and equipment needed for completing the actions described in the approved security plans and licensee protective strategy are readily available and in working condition.

(4) The licensee shall describe in the approved security plans, procedures for responding to an unplanned incident that reduces the number of available armed response team members below the minimum number documented by the licensee in the approved security plans.

(5) Protective Strategy. Licensees shall develop, maintain, and implement a written protective strategy in accordance with the requirements of this section and appendix C to this part.

(6) The licensee shall ensure that all personnel authorized unescorted access to the protected area are trained and understand their roles and responsibilities during security incidents, to include hostage and duress situations.

(7) Upon receipt of an alarm or other indication of threat, the licensee shall:

(i) Determine the existence of a threat in accordance with assessment procedures.

(ii) Identify the level of threat present through the use of assessment methodologies and procedures.

(iii) Determine the response necessary to intercept, challenge, delay, and neutralize the threat in accordance with the requirements of appendix C to part 73, the Commission-approved safeguards contingency plan, and the licensee response strategy.

(iv) Notify offsite support agencies such as local law enforcement, in accordance with site procedures.

(8) Law enforcement liaison. The licensee shall document and maintain current

agreements with local, state, and Federal law enforcement agencies, to include estimated response times and capabilities.

(l) Facilities using mixed-oxide (MOX) fuel assemblies. In addition to the requirements described in this section for protection against radiological sabotage, operating commercial nuclear power reactors licensed under 10 CFR parts 50 or 52 and using special nuclear material in the form of MOX fuel assemblies shall protect unirradiated MOX fuel assemblies against theft or diversion.

(1) Licensees shall protect the unirradiated MOX fuel assemblies against theft or diversion in accordance with the requirements of this section and the approved security plans.

(2) Commercial nuclear power reactors using MOX fuel assemblies are exempt from the requirements of §§ 73.20, 73.45, and 73.46 for the physical protection of unirradiated MOX fuel assemblies.

(3) Administrative controls.

(i) The licensee shall describe in the approved security plans, the operational and administrative controls to be implemented for the receipt, inspection, movement, storage, and protection of unirradiated MOX fuel assemblies.

(ii) The licensee shall implement the use of tamper-indicating devices for unirradiated MOX fuel assembly transport and shall verify their use and integrity before receipt.

(iii) Upon delivery of unirradiated MOX fuel assemblies, the licensee shall:

(A) Inspect unirradiated MOX fuel assemblies for damage.

(B) Search unirradiated MOX fuel assemblies for unauthorized materials.

(iv) The licensee may conduct the required inspection and search functions simultaneously.

(v) The licensee shall ensure the proper placement and control of unirradiated MOX fuel assemblies as follows:

(A) At least one armed security officer, in addition to the armed response team required by paragraphs (h)(4) and (h)(5) of appendix C to part 73, shall be present during the receipt and inspection of unirradiated MOX fuel assemblies.

(B) The licensee shall store unirradiated MOX fuel assemblies only within a spent fuel pool, located within a vital area, so that access to the unirradiated MOX fuel assemblies requires passage through at least three physical barriers.

(vi) The licensee shall implement a material control and accountability program for the unirradiated MOX fuel assemblies that includes a predetermined and documented storage location for each unirradiated MOX fuel assembly.

(vii) Records that identify the storage locations of unirradiated MOX fuel assemblies are considered safeguards information and must be protected and stored in accordance with § 73.21.

(4) Physical controls.

(i) The licensee shall lock or disable all equipment and power supplies to equipment required for the movement and handling of unirradiated MOX fuel assemblies.

(ii) The licensee shall implement a two-person line-of-sight rule whenever control systems or equipment required for the movement or handling of unirradiated MOX fuel assemblies must be accessed.

(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.

(3) Policies, requirements, and procedures.

(i) The licensee shall apply cyber-security requirements and policies that identify management expectations and requirements for the protection of computer systems.

(ii) The licensee shall develop and maintain implementing procedures to ensure cyber-security requirements and policies are implemented effectively.

(4) Incident response and recovery.

(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.

(ii) The cyber-security incident response and recovery plan must be described in the integrated response plan required by appendix C to this part.

(iii) The cyber-security incident response and recovery plan must ensure the capability to respond to cyber-security incidents, minimize loss and destruction, mitigate and correct the weaknesses that were exploited, and restore systems and/or equipment affected by a cyber-security incident.

(5) Protective strategies. The licensee shall implement defense-in-depth protective strategies to protect computer systems from cyber attacks, detecting, isolating, and neutralizing unauthorized activities in a timely manner.

(6) Configuration and control management program. The licensee shall implement a configuration and control management program, to include cyber risk analysis, to ensure that

modifications to computer system designs, access control measures, configuration, operational integrity, and management process do not adversely impact facility safety, security, and emergency preparedness systems before implementation of those modifications.

(7) Cyber-security awareness and training.

(i) The licensee shall implement a cyber-security awareness and training program.

(ii) The cyber-security awareness and training program must ensure that appropriate plant personnel, including contractors, are aware of cyber-security requirements and that they receive the training required to effectively perform their assigned duties and responsibilities.

(n) Security program reviews and audits.

(1) The licensee shall review the physical protection program at intervals not to exceed 12 months, or

(i) As necessary based upon assessments or other performance indicators.

(ii) Within 12 months after a change occurs in personnel, procedures, equipment, or facilities that potentially could adversely affect security.

(2) As a minimum, each element of the onsite physical protection program must be reviewed at least every twenty-four (24) months.

(i) The onsite physical protection program review must be documented and performed by individuals independent of those personnel responsible for program management and any individual who has direct responsibility for implementing the onsite physical protection program.

(ii) Onsite physical protection program reviews and audits must include, but not be limited to, an evaluation of the effectiveness of the approved security plans, implementing procedures, response commitments by local, state, and Federal law enforcement authorities, cyber-security programs, safety/security interface, and the testing, maintenance, and calibration program.

(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.

(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.

(5) The licensee shall conduct quarterly drills and annual force-on-force exercises in accordance with appendix C to part 73 and the licensee performance evaluation program.

(6) The results and recommendations of the onsite physical protection program reviews and audits, management's findings regarding program effectiveness, and any actions taken as a result of recommendations from prior program reviews, must be documented in a report to the licensee's plant manager and to corporate management at least one level higher than that having responsibility for day-to-day plant operation.

(7) Findings from onsite physical protection program reviews, audits, and assessments must be entered into the site corrective action program and protected as safeguards information, if applicable.

(8) The licensee shall make changes to the approved security plans and implementing procedures as a result of findings from security program reviews, audits, and assessments, where necessary to ensure the effective implementation of Commission regulations and the licensee protective strategy.

(9) Unless otherwise specified by the Commission, onsite physical protection program reviews, audits, and assessments may be conducted up to thirty days prior to, but no later than thirty days after the scheduled date without adverse impact upon the next scheduled annual audit date.

(o) Maintenance, testing, and calibration.

(1) The licensee shall:

(i) Implement a maintenance, testing and calibration program to ensure that security systems and equipment are tested for operability and performance at predetermined intervals, are maintained in operable condition, and are capable of performing their intended function when needed.

(ii) Describe the maintenance, testing and calibration program in the approved physical security plan. Implementing procedures must specify operational and technical details required to perform maintenance, testing, and calibration activities to include, but not limited to, purpose of activity, actions to be taken, acceptance criteria, the intervals or frequency at which the activity will be performed, and compensatory actions required.

(iii) Document problems, failures, deficiencies, and other findings, to include the cause of each, and enter each into the site corrective action program. The licensee shall protect this information as safeguards information, if applicable.

(iv) Implement compensatory measures in a timely manner to ensure that the effectiveness of the onsite physical protection program is not reduced by failure or degraded operation of security-related components or equipment.

(2) Each intrusion alarm must be tested for operability at the beginning and end of any period that it is used for security, or if the period of continuous use exceeds seven (7) days, the intrusion alarm must be tested at least once every seven (7) days.

(3) Intrusion detection and access control equipment must be performance tested in accordance with the approved security plans.

(4) Equipment required for communications onsite must be tested for operability not less frequently than once at the beginning of each security personnel work shift.

(5) Communication systems between the alarm stations and each control room, and between the alarm stations and offsite support agencies, to include back-up communication equipment, must be tested for operability at least once each day.

(6) Search equipment must be tested for operability at least once each day and tested for performance at least once during each seven (7) day period and before being placed back in service after each repair or inoperative state.

(7) All intrusion detection equipment, communication equipment, physical barriers, and other security-related devices or equipment, to include back-up power supplies must be maintained in operable condition.

(8) A program for testing or verifying the operability of devices or equipment located in hazardous areas must be specified in the approved security plans and must define alternate measures to be taken to ensure the timely completion of testing or maintenance when the hazardous condition or radiation restrictions are no longer applicable.

(p) Compensatory measures.

(1) The licensee shall identify measures and criteria needed to compensate for the loss or reduced performance of personnel, equipment, systems, and components, that are required to meet the requirements of this section.

(2) Compensatory measures must be designed and implemented to provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable personnel, equipment, system, or components.

(3) Compensatory measures must be implemented within specific time lines necessary to meet the requirements stated in paragraph (b) of this section and described in the approved security plans.

(q) Suspension of safeguards measures.

(1) The licensee may suspend implementation of affected requirements of this section under the following conditions:

(i) In accordance with §§ 50.54(x) and 50.54(y) of this chapter, the licensee may suspend any safeguards measures pursuant to this section in an emergency when this action is

immediately needed to protect the public health and safety and no action consistent with license conditions and technical specifications that can provide adequate or equivalent protection is immediately apparent. This suspension of safeguards measures must be approved as a minimum by a licensed senior operator prior to taking this action.

(ii) During severe weather when the suspension is immediately needed to protect personnel whose assigned duties and responsibilities in meeting the requirements of this section would otherwise constitute a life threatening situation and no action consistent with the requirements of this section that can provide equivalent protection is immediately apparent. Suspension of safeguards due to severe weather must be initiated by the security supervisor and approved by a licensed senior operator prior to taking this action.

(2) Suspended security measures must be reimplemented as soon as conditions permit.

(3) The suspension of safeguards measures must be reported and documented in accordance with the provisions of § 73.71.

(4) Reports made under § 50.72 of this chapter need not be duplicated under § 73.71.

(r) Records.

(1) The Commission may inspect, copy, retain, and remove copies of all records required to be kept by Commission regulations, orders, or license conditions whether the records are kept by the licensee or a contractor.

(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.

(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.

(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 of this chapter 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

(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.

15. A new § 73.62 is added to read as follows:

§ 73.62 Security assessment for nuclear power plants.

(a) *Definitions*.

Security design features means structures, systems and components of a nuclear power plant and their layout that are relied upon to either–

(i) Detect, delay, assess, or respond to an attack against target sets of a nuclear power plant by an adversary possessing the characteristics of the design basis threat;

(ii) Mitigate the effects of such an attack; or

(iii) Mitigate the effects of circumstances associated with a loss of large areas of the facility due to explosions or fires.

Security functions means those functions necessary to–

(i) Detect, delay, assess, or respond to an attack against target sets of a nuclear power plant by an adversary possessing the characteristics of the design basis threat;

(ii) Mitigate the effects of such an attack; or

(iii) Mitigate the effects of circumstances associated with loss of large areas of the facility due to explosions or fires. Security functions may be accomplished through security design features or by the operational programs as described in the physical security, training and qualification, and contingency plans (security plans) under § 73.55.

Security assessment parameters means–

(i) The characteristics or parameters of a site where the nuclear power plant or reactor is to, or may, be utilized, either as postulated in the security assessment or as identified in accordance with 10 CFR 100.21(f);

(ii) Security design features which are outside the scope of the design being addressed at the particular stage of the regulatory process, which are postulated in a security assessment; and

(iii) Features of a physical security program under § 73.55 which are postulated in a security assessment.

(b) *Security assessment*. Each applicant for a construction permit, operating license, or standard design approval for a nuclear power plant under part 50 of this chapter; a standard design certification under subpart B of part 52 of this chapter; a combined license under subpart C of part 52; a standard design approval under part 52, or a manufacturing license under appendix M of part 52, whose application is filed after [THE EFFECTIVE DATE OF RULE] shall perform a security assessment of the reactor or facility design (within the scope of design being addressed at the particular stage of the regulatory process). The security assessment must:

(1) Identify target sets.

(2) Apply a risk evaluation methodology for selected scenarios to determine the effectiveness of candidate security design features in accomplishing security functions.

(3) Use security assessment parameters to evaluate candidate security design features when site characteristics or security operational programs are not yet determined; and

(4) Use a systematic screening process, to determine the practicability of these candidate security design features for inclusion in the facility. The process must consider safety interface, security optimization and cost-effectiveness.

(c) *Contents of security assessment*. The security assessment must include each of the matters identified below.

(1) A description of the process to develop and identify target sets, including analyses and methodologies used to determine and group the target set equipment;

(2) A list of the target sets;

(3) A description of the methodologies used in the assessment, including the screening process for practicability decisions on security design features;

(4) The security functions for the plant;

(5) The security design features incorporated into the design, together with an explanation of how each security design feature provides or enhances the capability of the plant to protect the target sets against an adversary possessing the characteristics of the design basis threat, or to mitigate the effects of circumstances associated with loss of large areas of the facility due to explosions or fires;

(6) The security assessment parameters used in the assessment (including those identified from the security assessment conducted at the construction permit, standard design approval, design certification, or manufacturing stage, as applicable); and

(7) Security assessment parameters to be considered in the security design assessments for future design stages (as applicable), and in the development of the security plans required under § 73.55.

(d)–(e) [Reserved]

(f) *Incorporation of security design features into the design*. Each standard design approval, standard design certification, construction permit, operating license, combined license, and manufacturing license whose applications are filed after [EFFECTIVE DATE OF RULE] must assure, within the scope of design being addressed at the particular stage of the regulatory process, that practicable security design features have been integrated into the facility.

(g) *Inclusion of security design features in security operational programs.* Each operating license, combined license, and manufacturing license whose applications are filed after [EFFECTIVE DATE OF RULE] must assure that practicable security design features, identified during the assessment process, and information about the functions they perform are integrated into the security plans required by § 73.55 and associated appendices.

Dated at Rockville, Maryland, this day of , 2006.

For the Nuclear Regulatory Commission.

Annette Vietti-Cook,

Secretary of the Commission.