[7590-01-P]

NUCLEAR REGULATORY COMMISSION

10 CFR Parts 50, 52, 72, and 73

[NRC-2008-0019]

RIN 3150-AG63

Power Reactor Security Requirements

**AGENCY**: Nuclear Regulatory Commission.

**ACTION**: Final rule.

**SUMMARY**: The Nuclear Regulatory Commission (NRC) is amending its security regulations and adding new security requirements pertaining to nuclear power reactors. This rulemaking establishes and updates generically applicable security requirements similar to those previously imposed by Commission orders issued after the terrorist attacks of September 11, 2001. Additionally, this rulemaking adds several new requirements not derived directly from the security order requirements but developed as a result of insights gained from implementation of the security orders, review of site security plans, implementation of the enhanced baseline inspection program, and NRC evaluation of force-on-force exercises. This rulemaking also updates the NRC's security regulatory framework for the licensing of new nuclear power plants. Finally, it resolves three petitions for rulemaking (PRM) that were considered during the development of the final rule.

**DATES**: *Effective Date:* This final rule is effective on **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].** *Compliance Date*: Compliance with this final rule is required by **[INSERT DATE 180 DAYS AFTER EFFECTIVE DATE]** for licensees currently licensed to operate under 10 CFR part 50**.**

ADDRESSES: You can access publicly available documents related to this document using the following methods:

**Federal e-Rulemaking Portal:** Go to http://www.regulations.gov and search for documents filed under Docket ID [NRC-2008-0019]. Address questions about NRC Dockets to Carol Gallagher at 301-415-5905; e-mail Carol.Gallagher@nrc.gov.

**NRC's Public Document Room (PDR):** The public may examine and have copied for a fee publicly available documents at the NRC's PDR, Public File Area O1 F21, One White Flint North, 11555 Rockville Pike, Rockville, Maryland.

**NRC's Agency Wide Documents Access and Management System (ADAMS):** Publicly available documents created or received at the NRC are available electronically at the NRC's Electronic Reading Room at http://www.nrc.gov/reading-rm/adams.html. From this page, the public can gain entry into ADAMS, which provides text and image files of the NRC's public documents. If you do not have access to ADAMS or if there are problems in accessing the documents located in ADAMS, contact the NRC's PDR reference staff at 1-800-397-4209, 301-415-4737 or by e-mail to pdr.resource@nrc.gov.

**FOR FURTHER INFORMATION CONTACT:** Ms. Bonnie Schnetzler, Office of Nuclear Security and Incident Response, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001; telephone 301-415-7883; e-mail: Bonnie.Schnetzler@nrc.gov, or Mr. Timothy Reed, Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001; telephone 301-415-1462; e-mail: Timothy.Reed@nrc.gov.

**SUPPLEMENTARY INFORMATION:**

I. Background.

II. Petitions for Rulemaking.

III. Discussion of Substantive Changes and Responses to Significant Comments.

IV. Section-by-Section Analysis.

V. Guidance.

VI. Criminal Penalties.

VII. Availability of Documents.

VIII. Voluntary Consensus Standards.

IX. Finding of No Significant Environmental Impact.

X. Paperwork Reduction Act Statement.

XI. Regulatory Analysis.

XII. Regulatory Flexibility Certification.

XIII. Backfit Analysis.

XIV. Congressional Review Act.

## I. Background.

### A. Historical Background and Overview.

Following the terrorist attacks on September 11, 2001, the Commission issued a series of orders to ensure that nuclear power plants and other licensed facilities continued to have effective security measures in place given the changing threat environment. Through these orders, the Commission supplemented the design basis threat (DBT) as well as mandated specific training enhancements, access authorization enhancements, and enhancements to defensive strategies, mitigative measures, and integrated response. Additionally, through

generic communications, the Commission specified expectations for enhanced notifications to the NRC for certain security events or suspicious activities. The four following security orders were issued to licensees:

- EA-02-026, "Interim Compensatory Measures (ICM) Order," issued February 25, 2002 (March 4, 2002; 67 FR 9792);
- EA-02-261, "Access Authorization Order," issued January 7, 2003 (January 13, 2003; 68 FR 1643);
- EA-03-039, "Security Personnel Training and Qualification Requirements (Training) Order," issued April 29, 2003 (May 7, 2003; 68 FR 24514); and
- EA-03-086, “Revised Design Basis Threat Order,” issued April 29, 2003 (May 7, 2003; 68 FR 24517).

Nuclear power plant licensees revised their physical security plans, access authorization programs, training and qualification plans, and safeguards contingency plans in response to these orders. The Commission completed its review and approval of the revised security plans on October 29, 2004. These plans incorporated the enhancements required by the orders. While the specifics of these enhancements are protected as Safeguards Information consistent with 10 CFR 73.21, the enhancements resulted in measures such as increased patrols; augmented security forces and capabilities; additional security posts; additional physical barriers; vehicle checks at greater standoff distances; enhanced coordination with law enforcement authorities; augmented security and emergency response training, equipment, and communication; and more restrictive site access controls for personnel including expanded, expedited, and more thorough employee background investigations.

The Energy Policy Act of 2005 (EPAct 2005), signed into law on August 8, 2005, contained several provisions relevant to security at nuclear power plants. Section 653, for instance, added Section 161A. to the Atomic Energy Act of 1954, as amended (AEA). This

provision allows the Commission to authorize certain licensees to use, as part of their protective strategies, an expanded arsenal of weapons including machine guns and semi-automatic assault weapons. Section 653 also requires certain security personnel to undergo a background check that includes fingerprinting and a check against the Federal Bureau of Investigation's (FBI) National Instant Criminal Background Check System (NICS) database. Section 161A, however, is not effective until guidelines are completed by the Commission and approved by the Attorney General. More information on the NRC's implementation of Section 161A. can be found below.

**B. The Proposed Rule**.

As noted to recipients of the post-September 11, 2001, orders, it was always the Commission's intent to complete a thorough review of the existing physical protection program requirements and undertake a rulemaking that would codify generically-applicable security requirements. This rulemaking would be informed by the requirements previously issued by orders and includes an update of existing power reactor security requirements, which had not been significantly revised for nearly 30 years. To that end, on October 26, 2006, the Commission issued the proposed Power Reactor Security rulemaking (71 FR 62663). The proposed rule was originally published for a 75-day public comment period. In response to several requests for extension, the comment period was extended on two separate occasions (January 5, 2005; 72 FR 480; and February 28, 2007; 72 FR 8951), eventually closing on March 26, 2007. The Commission received 48 comment letters. In addition, the Commission held two public meetings to solicit public comment in Rockville, MD on November 15, 2006, and Las Vegas, NV on November 29, 2006. The Commission held a third public meeting in Rockville, MD, on March 9, 2007, to facilitate stakeholder understanding of the proposed requirements, and thereby result in more informed comments on the proposed rule provisions.

In addition to proposing requirements that were similar to those that had previously

been imposed by the various orders, the proposed rule also contained several new provisions that the Commission determined would provide additional assurance of licensee capabilities to protect against the DBT. These new provisions were identified by the Commission during implementation of the security orders while reviewing the revised site security plans that had been submitted by licensees for Commission review and approval, while conducting the enhanced baseline inspection program, and through evaluation of the results of force-on-force exercises. As identified in the proposed rule, these new provisions included such measures as cyber security requirements, safety/security interface reviews, functional equivalency of the central and secondary alarm stations, uninterruptable backup power for detection and assessment equipment, and video image recording equipment (See 71 FR 62666-62667; October 26, 2006).

The Commission also published a supplemental proposed rule on April 10, 2008 (73 FR 19443) seeking additional stakeholder comment on two provisions of the rule for which the Commission had decided to provide additional detail. The supplemental proposed rule also proposed to move these requirements from appendix C to part 73 in the proposed rule to §50.54 in the final rule. More detail on those provisions and the comments received is provided in section III of this document.

Three petitions for rulemaking (PRM) (PRM-50-80, PRM-73-11, PRM-73-13) were also considered as part of this rulemaking. Consideration of these petitions is discussed in detail in section II of this document.

**C. Significant New Requirements in the Final Rule**.

This final rulemaking amends the security requirements for power reactors. The following existing sections and appendices in 10 CFR Part 73 have been revised as a result:

- 10 CFR 73.55, Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.
- 10 CFR 73.56, Personnel access authorization requirements for nuclear power

plants.

- 10 CFR Part 73, appendix B, section VI, Nuclear Power Reactor Training and Qualification Plan for Personnel Performing Security Program Duties.
- 10 CFR Part 73, appendix C, Licensee Safeguards Contingency Plans.

The amendments also add two new sections to part 73 and a new paragraph to 10 CFR part 50:

- 10 CFR 73.54, Protection of digital computer and communication systems and networks (i.e., cyber security requirements).
- 10 CFR 73.58, Safety/security interface requirements for nuclear power reactors.
- 10 CFR 50.54(hh), mitigative strategies and response procedures for potential or actual aircraft attacks.

Specifically, this rulemaking contains a number of significant new requirements listed as follows:

Safety/Security Interface Requirements. These requirements are located in new § 73.58. The safety/security interface requirements explicitly require licensees to manage and assess the potential conflicts between security activities and other plant activities that could compromise either plant security or plant safety. The requirements direct licensees to assess and manage these interactions so that neither safety nor security is compromised. These requirements address, in part, PRM-50-80, which requested the establishment of regulations governing proposed changes to the facilities which could adversely affect the protection against radiological sabotage.

Mixed-Oxide (MOX) Fuel Requirements. These requirements are codified into new § 73.55(l) for reactor licensees who propose to use MOX fuel in concentrations of 20 percent or less. These requirements provide enhancements to the normal radiological sabotage-based physical security requirements by adding the requirement that the MOX fuel be protected from

theft or diversion. These requirements reflect the Commission's view that the application of security requirements for the protection of formula quantities of strategic special nuclear material set forth in Part 73, which would otherwise apply because of the MOX fuel's plutonium content, is, in part, unnecessary to provide adequate protection for this material because of the weight and size of the MOX fuel assemblies. The MOX fuel security requirements are consistent with the approach implemented at Catawba Nuclear Station through the MOX lead test assembly effort in 2004-2005.

Cyber Security Requirements. These requirements are codified as new § 73.54 and designed to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks up to and including the design basis threat as established by § 73.1(a)(1)(v). These requirements are substantial improvements upon the requirements imposed by the February 25, 2002, order. In addition to requiring that all new applications for an operating or combined license include a cyber security plan, the rule will also require currently operating licensees to submit a cyber security plan to the Commission for review and approval by way of license amendment pursuant to § 50.90 within 180 days of the effective date of this final rule. In addition, applicants who have submitted an application for an operating license or combined license currently under review by the Commission must amend their applications to include a cyber security plan. For both current and new licensees, the cyber security plan will become part of the licensee's licensing basis in the same manner as other security plans.

Mitigative Strategies and Response Procedures for Potential or Actual Aircraft Attacks. These requirements appear in new § 50.54(hh). Section 50.54(hh)(1) establishes the necessary regulatory framework to facilitate consistent application of Commission requirements for preparatory actions to be taken in the event of a potential or actual aircraft attack and mitigation strategies for loss of large areas due to fire and explosions. Section 50.54(hh)(2) requires

licensees to develop guidance and strategies for addressing the loss of large areas of the plant due to explosions or fires from a beyond-design basis event through the use of readily available resources and identification of potential practicable areas for the use of beyond-readily-available resources. Requirements similar to these were previously imposed under section B.5 of the February 25, 2002, ICM order; specifically, the "B.5.a" and the "B.5.b" provisions.

Access Authorization Enhancements. Section 73.56 has been substantially revised to incorporate lessons learned from the Commission's implementation of the January 7, 2003, order requirements and to improve the integration of the access authorization and security program requirements. The final rule includes an increase in the rigor for many elements of the pre-existing access authorization program requirements. In addition, the access authorization requirements include new requirements for individuals who have electronic means to adversely impact facility safety, security, or emergency preparedness; enhancements to the psychological assessments requirements; requires information sharing between reactor licensees; expanded behavioral observation requirements; requirements for reinvestigations of criminal and credit history records for all individuals with unescorted access; and 5-year psychological reassessments for certain critical job functions.

Training and Qualification Enhancements. These requirements are set forth in appendix B to part 73 and include modifications to training and qualification program requirements based on insights gained from implementation of the security orders, Commission reviews of site security plans, implementation of the enhanced baseline inspection program, and insights gained from evaluations of force-on-force exercises. These new requirements include additional requirements for unarmed security personnel to assure these personnel meet minimum physical requirements commensurate with their duties. The new requirements also include a minimum age requirement of 18 years for unarmed security officers, enhanced minimal qualification scores for testing required by the training and qualification plan, enhanced

qualification requirements for security trainers, armorer certification requirements, program requirements for on-the-job training, and qualification requirements for drill and exercise controllers.

Physical Security Enhancements. The rule imposes new physical security enhancements in the revised § 73.55 that were identified by the Commission during implementation of the security orders, reviews of site security plans, implementation of the enhanced baseline inspection program, and NRC evaluations of force-on-force exercises. Significant new requirements in § 73.55 include a requirement that the central alarm station (CAS) and secondary alarm station (SAS) have functionally equivalent capabilities so that no single act in accordance with the design basis threat of radiological sabotage could disable the key functions of both CAS and SAS. Additions also include requirements for new reactor licensees to locate the SAS within a site's protected area, ensure that the SAS is bullet resistant, and limit visibility into the SAS from the perimeter of the protected area. Revisions to § 73.55 also include requiring uninterruptible backup power supplies for detection and assessment equipment, video image recording capability, and new requirements for protection of the facility against waterborne vehicles.

**D. Significant Changes in the Final Rule**.

A number of significant changes were made to the proposed rule as a result of public comments, and they are now reflected in the final rule. Those changes are outlined as follows:

Separation of Enhanced Weapons and Firearms Background Check Requirements. As noted previously, Section 161A of the AEA permits the Commission to authorize the use of certain enhanced weapons in the protective strategies of certain designated licensees once guidelines are developed by the Commission and approved by the Attorney General. In anticipation of the completion of those guidelines and the Attorney General's approval, the Commission had included in the proposed rule several provisions that would implement its

proposed requirements concerning application for and approval of the use of enhanced weapons and firearms background checks. However, because the guidelines had not yet received the approval of the Attorney General as the final rule was submitted to the Commission, the Commission decided to address that portion of the proposed rule in a separate rulemaking. Once the final guidelines are approved by the Attorney General and published in the *Federal Register*, the Commission will take appropriate action to codify the Section 161A. authorities.

Cyber Security Requirements. Another change to this final rulemaking is the relocation of cyber security requirements. Cyber security requirements had been located in the proposed rule in § 73.55(m). These requirements are now placed in new § 73.54 as a separate section within part 73. These requirements were placed in a stand-alone section to enable the cyber security requirements to be made applicable to other types of facilities and applications through future rulemakings.

Establishing these requirements as a stand-alone section also necessitated creating accompanying licensing requirements. Because the cyber security requirements were originally proposed as part of the physical security program and thus the physical security plan, a licensee's cyber security plan under the proposed rule would have been part of the license through that licensing document. Once these requirements were separated from proposed § 73.55, the Commission identified the need to establish separate licensing requirements for the licensee's cyber security plan that would require the plan to be part of a new application for a license issued under part 50 or part 52, as well as continue to be a condition of either type of license. Conforming changes were therefore made to sections §§ 50.34, 50.54, 52.79, and 52.80 to address this consideration. As noted previously and in § 73.54, for current reactor licensees, the rule requires the submission of a new cyber security plan to the Commission for review and approval within 180 days of the effective date of the final rule. Current licensees are required to submit their cyber security plans by way of a license amendment pursuant to 10 CFR § 50.90. In addition, applicants for an operating license or combined license who have

submitted their applications to the Commission prior to the effective date of the rule are required to amend their applications to the extent necessary to address the requirements of § 73.54.

Performance Evaluation Program Requirements. The Performance Evaluation Program requirements that were in proposed appendix C to part 73, are moved in their entirety to appendix B to part 73 as these requirements describe the development and implementation of a training program for training the security force in the response to contingency events.

Mitigative Strategies and Response Procedures for Potential or Actual Aircraft Attacks. Another significant change to this rulemaking is the relocation of and the addition of clarifying rule language to the beyond-design basis mitigative measures and potential aircraft threat notification requirements that were previously located in proposed part 73, appendix C. Those requirements are now set forth in 10 CFR 50.54(hh). This change was made, in part, in response to stakeholder comments that part 73, appendix C, was not the appropriate location for these requirements because the requirements were not specific to the licensee's security organization. The Commission agreed and relocated the requirements accordingly and provided more details to the final rule language to ensure that the intent of these requirements is clear. As noted previously, the Commission issued a supplemental proposed rule seeking additional stakeholder comment on these proposed changes to the rule. More detail on this provision is provided in Section III of this document.

Section 73.71 and Appendix G to Part 73. The proposed power reactor security rulemaking contained proposed requirements for § 73.71 and appendix G to part 73. Based on public comments, the Commission intended to make few changes to these regulations. However, these provisions are not contained in this final rulemaking. Because the enhanced weapons rulemaking (discussed previously) will include potential changes to § 73.71 and appendix G to part 73, the Commission decided that revisions to these regulations were better suited for that rulemaking.

Security Plan Submittal Requirements. The proposed rule would have required current

licensees to revise their physical security plan, training and qualification plans, and safeguards contingency plan to incorporate the new requirements and to submit these security plans for Commission review and approval. The final rule no longer requires these security plans (with the exception of the cyber security plan as discussed previously) to be submitted for prior Commission review and approval and instead allows licensees to make changes in accordance with existing licensing provisions such as § 50.54(p) or § 50.90, as applicable. The Commission determined that this was an acceptable approach because most of the requirements established by this rule are substantially similar to the requirements that had been imposed by the security orders and because all licensee security plans were recently reviewed and approved by the Commission in 2004 following issuance of those orders. Additionally, many of the additional requirements in the final rule are already current practices that were implemented following an industry-developed, generic, security plan template that was reviewed and approved by the Commission. For the requirements that go beyond current practices, the Commission does not expect that changes required by this rule would result in a decrease of effectiveness in a licensee's security plan. For implementation of those new requirements, licensees should, therefore, consider whether their plans could be revised in accordance with the procedures described in § 50.54(p). However, if a licensee believes that a plan change may reduce the effectiveness of a security plan or if the licensee desires Commission review and approval of the plan change, then the proposed plan revision should be submitted to the NRC for review and approval as a license amendment per § 50.90.

With respect to applicants who have already submitted an application to the Commission for an operating license or combined license as of the effective date of this rule, those applicants are required by this rule to amend their applications to the extent necessary to address the requirements of the new rule.

Implementation of the Final Rule. The staff recommends that the final rule be effective 30 days following date of publication. This would permit applicability of the rule's requirements

to new reactor applicants at the earliest possible date. However, the staff also recommends that a separate compliance date be specified for current licensees so that those licensees would be not be required to be in compliance with the rule requirements until 180 days following the effective date of the rule.

Definitions. The proposed rule contained a number of definitions, primarily related to the proposed enhanced weapons requirements. As noted previously, the enhanced weapons provisions and firearms backgrounds checks have been separated into a separate rulemaking so codifying those definitions is no longer appropriate in this rulemaking. Regarding the other proposed rule definitions of safety/security interface, security officer, and target sets, the NRC staff recommends that these terms be addressed in guidance, and accordingly the final rule does not contain these definitions.

EPAct 2005 Provisions. As noted above, the proposed rule contained a number of proposed requirements that were designed to address security-related provisions of the EPAct 2005. With respect to Section 653 of the EPAct 2005, enhanced weapons and firearms background check requirements have been moved to a separate rulemaking. The only other provisions of the EPAct 2005 that the Commission had considered during this rulemaking were in Section 651, which concerns matters related to the triennial Commission-evaluated, force-on-force exercises, the NRC's mitigation of potential conflicts of interest in the conduct of such exercises, and the submission of annual reports by the NRC to Congress. Because the statute requires the NRC to be directly responsible for implementation of those requirements, the Commission has determined that there is no need for them to be specifically reflected in the NRC's regulations. The NRC has fully complied with all of the requirements of Section 651 in its conduct of force-on-force evaluations since the EPAct 2005, and has submitted three annual reports to Congress during that time. Further discussion of and the Commission's response to a comment on this issue are provided below in Section III.

**E. Conforming and Corrective Changes**.

Conforming changes to the requirements listed below are made to ensure that cross-referencing between the various security regulations in part 73 is preserved, implement cyber security plan submittal requirements, and preserve requirements for licensees who are not within the scope of this final rule. The following requirements contain conforming changes:

- Section 50.34, "Contents of construction permit and operating license applications; technical information," is revised to align the application requirements with appendix B to 10 CFR part 73, the addition of § 73.54 to part 73, and the addition of § 50.54(hh) to part 50.
- Section 50.54, "Conditions of licenses," is revised to conform with the revisions to sections in appendix C to 10 CFR part 73. In accordance with the introductory text to §50.54, revisions to this section are also made applicable to combined licenses issued under part 52.
- Section 52.79, "Contents of applications; technical information in the final safety analysis report," is revised to align the application requirements with the revisions to appendix C to 10 CFR part 73 and the addition of § 73.54 to part 73.
- Section 52.80, "Contents of applications; additional technical information," is revised to add the application requirements for § 50.54(hh) to part 50.
- Section 72.212, "Conditions of general license issued under § 72.210," is revised to reference the appropriate revised paragraph designations in § 73.55.
- Section 73.8, "Information collection requirements: OMB approval," is revised to add the new requirements (§§ 73.54 and 73.58) to the list of sections with Office of Management and Budget (OMB) information collection requirements. A corrective revision to § 73.8 is made to reflect OMB approval of existing information collection requirements for NRC Form 366 under existing § 73.71.
- Section 73.70, "Records," is revised to reference the appropriate revised paragraph designations in § 73.55 regarding the need to retain a record of the registry of

visitors.

Additionally, § 73.81, “Criminal penalties,” which sets forth the sections within part 73 that are not subject to criminal sanctions under the AEA, would remain unchanged because willful violations of the new §§ 73.54 and 73.58 may be subject to criminal sanctions.

Appendix B to part 73 and appendix C to part 73 require special treatment in this final rule to preserve, with a minimum of conforming changes, the current requirements for licensees and applicants who are not within the scope of this final rule, such as Category I strategic special nuclear material licensees and research and test reactor licensees. Accordingly, Sections I through V of appendix B to part 73 remain unchanged to preserve the current training and qualification requirements for all applicants, licensees, and certificate holders who are not within the scope of this final rule, and the new language for power reactor security training and qualification (revised in this final rule) is added as Section VI. Part 73, appendix C, is divided into two sections, with Section I maintaining all current requirements for licensees and applicants not within the scope of this final rule, and Section II containing all new requirements related to power reactor contingency response.

## II. Petitions for Rulemaking.

Three petitions for rulemaking were considered during the development of the final rule requirements consistent with previous petition resolution and closure process for these petitions (i.e., PRM-50-80, PRM-73-11, and PRM-73-13). All three petitions are closed, and the discussion that follows provides the Commission's consideration of the issues raised in each petition as part of the development of the final power reactor security requirements.

### A. PRM-50-80.

PRM-50-80, submitted by the Union of Concerned Scientists (UCS) and the San Luis Obispo Mothers for Peace (SLOMFP), was published for public comment on June 16, 2003 (68 FR 35568). The petition requested that the Commission take two actions. The first action

was to amend 10 CFR 50.54(p), “Conditions of licenses,” and 10 CFR 50.59, “Changes, tests, and experiments,” to require licensees to evaluate whether proposed changes, tests, or experiments cause protection against radiological sabotage to be decreased and, if so, to conduct such actions only with prior Commission approval. The second action requested that the Commission amend 10 CFR part 50 to require licensees to evaluate their facilities against specified aerial hazards and make necessary changes to provide reasonable assurance that the ability of the facility to reach and maintain safe shutdown would not be compromised by an accidental or intentional aerial assault. The second action (regarding aerial hazards) was previously considered and resolved as part of the final design basis threat (DBT) (§ 73.1) rulemaking (March 19, 2007; 72 FR 12705). On November 17, 2005 (70 FR 69690), the Commission decided to consider the petitioner’s first request for rulemaking (i.e., evaluation of proposed changes, tests, or experiments to determine whether radiological sabotage protection is decreased). Proposed language addressing the issues raised in the petition was published as proposed § 73.58, “Safety/security interface requirements for nuclear power reactors.” This section remains in the final rule. Refer to the section-by-section analysis in this document, supporting § 73.58 for further discussion of the safety/security interface requirements.

**B. PRM-73-11.**

PRM-73-11, submitted by Scott Portzline, Three Mile Island Alert, was published for public comment on November 2, 2001 (66 FR 55603). The comment period closed on January 16, 2002. Eleven comment letters were received. Of the 11 comments filed, 7 were from governmental organizations, 2 were from individuals, and 2 were from industry organizations. The majority of the comments support the petitioner’s recommendation.

The petitioner requested that the NRC regulations governing physical protection of plants and materials be amended to require NRC licensees to post at least one armed guard at each entrance to the ‘‘owner controlled areas’’ (OCA) surrounding all U.S. nuclear power plants. The petitioner stated that this should be accomplished by requiring the addition of armed site

protection officers (SPO) to the total number of SPOs —not by simply shifting SPOs from their protected area (PA) posts to the OCA entrances. The petitioner believes that the proposed amendment would provide an additional layer of security that would complement existing measures against radiological sabotage and would be consistent with the long-standing principle of defense-in-depth.

In a *Federal Register* Notice published December 27, 2006 (72 FR 481), the Commission informed the public that PRM-73-11 and the public comments filed on the petition would be considered in this final rule. Consideration of PRM-73-11 and the associated comments was undertaken as part of the effort to finalize the requirements governing security in the OCA.

The Commission has concluded that prescriptively requiring armed security personnel in the OCA is not necessary. Instead, the final physical security requirements in § 73.55(k) allows licensees the flexibility to determine the need for armed security personnel in the OCA, as a function of site-specific considerations, such that the licensee can defend against the DBT with high assurance. In reaching this determination, the Commission recognized that the requirements governing protective strategies must be more performance-based to enable licensees to adjust their strategies to address the site-specific circumstances and that a prescriptive requirement for armed security personnel in the owner controlled area may not always be the most effective approach for every licensee in defending against the DBT. The Commission constructed the final physical security requirements, recognizing the range of site-specific circumstances that exist, to put in place the performance objectives that must be met, and where possible, provided flexibility to licensees to construct strategies that meet the objectives.

**C. PRM-73-13.**

PRM-73-13, submitted by David Lochbaum, Union of Concerned Scientists, was published for public comment on April 9, 2007 (72 FR 17440) and the comment period closed

June 25, 2007.

The petitioner requested that the Commission amend part 73 to require that licensees implement procedures to ensure that, when information becomes known to a licensee about an individual seeking access to the protected area that would prevent that individual from gaining unescorted access to the protected area of a nuclear power plant, the licensee will implement measures to ensure the individual does not enter the protected area, whether escorted or not. Further, the petitioner requested that the NRC's regulations be amended to require that, when sufficient information is not available to a licensee about an individual seeking access to the protected area to determine whether the criteria for unescorted access are satisfied, the licensee will implement measures to allow that individual to enter the protected area only when escorted at all times by an armed member of the security force who maintains communication with security supervision.

The Commission determined that the issues raised in PRM-73-13 were appropriate for consideration and were in fact issues already being considered in the Power Reactor Security Requirements rulemaking. Accordingly, the issues raised by PRM-73-13 and the public comments received were considered as part of the effort to finalize the requirements that govern escort and access within the protected area (refer to requirements in § 73.55(g) and § 73.56(h) for the specific final rule requirements).

The Nuclear Energy Institute (NEI) commented on PRM-73-13, with 11 other industry organizations agreeing (hereafter referred to collectively as commenters). The commenters agreed that the petitioner's first request (with regard to preventing an individual to have access to the protected area when derogatory information becomes known) should be issued as a notice of proposed rulemaking. Neither NEI nor any of the other commenters commented on any of the specific language proposed by the petitioner. With regard to the second provision proposed by the petitioner (requiring armed escorts for certain visitors), the commenters did not agree with the proposal. The commenters argued that the use of trained individuals, though not

necessarily armed, in conjunction with search equipment and techniques as well as the limitation placed on visitors (i.e., that visitors must have a “work-related need” for entry into the PA) have resulted in no incidents that warrant imposing this new requirement.

The Commission has decided not to adopt either proposal. Regarding the petitioner’s second proposal, the Commission agrees with the commenters that the current protective measures for escorted personnel are sufficient to protect against the scenario presented by the petitioner. Licensee escorted access programs have been in place for years without incident, and the petitioner has not provided a basis that raises questions about their sufficiency.

With respect to the petitioner’s first proposal, the Commission does not agree that the NRC’s unescorted access requirements described in § 73.56 and § 73.57 need to contain prescriptive disqualifiers for access. Licensees are required by § 73.56(h) in this final rule to consider all of the information obtained in the background investigation for determining whether an individual is trustworthy and reliable before granting unescorted access. There is no particular piece of information obtained during a background investigation that would automatically disqualify an individual from access. This principle applies even to criminal history record information required to be considered by statute (Section 149 of the AEA) and by § 73.57. Accordingly, if no one piece of information obtained during a background investigation for suitability for individuals precludes granting unescorted access, there is no information that would automatically prevent the individual from gaining escorted access to the protected area as suggested by the petitioner. The final rule § 73.55(g)(7), however, does have several restrictions on escorted access (visitors) including verification of identity, verification of reason for business inside the protected area, and collection of information (visitor control register) pertaining to the visitor. In addition, there are several conditions that individuals who escort the visitor must adhere to including continuous monitoring of the visitor while inside the protected area, having a means of timely communication with security, and having received training on

escort duties. Lastly, licensees may not allow any individual who is currently denied access at any other facility to be a visitor.

Furthermore, the petitioner's suggested language that a licensee must act to deny escorted access when such information "becomes known to the licensee" is unworkable from a regulatory perspective. It is unclear what the NRC could impose on licensees as an enforceable standard for such a scenario. In order to avoid potential enforcement action, a licensee would be put in a position to conduct a full background investigation on a visitor each time access is requested, which would undermine the entire purpose behind having the ability to escort visitors on site, or, in accordance with the petitioner's second suggestion, assign an armed security officer to escort that individual. The Commission does not have a basis to impose either measure, and the petitioners have not provided a basis in support of it. Section 73.55(g), however, does not allow individuals currently denied access at other facilities to be a visitor.

## III. Discussion of Substantive Changes and Responses to Significant Comments.

### A. Introduction.

A detailed discussion of the public comments submitted on the proposed power reactor security rule and supplemental proposed rule as well as the Commission's responses are contained in a separate document (see Section VII, "Availability of Documents," of this document). This section discusses the more significant comments submitted on the proposed power reactor security provisions and the substantive changes made to develop the final power reactor security requirements.

The changes made to the power reactor security requirements are discussed by part, with changes to part 50 requirements being discussed first, followed by the changes to part 73 requirements, and proceeding in numerical order according to the section number. General topics are discussed first, followed by discussion of changes to individual sections as necessary.

In addition to the substantive changes, rule language was revised to make conforming administrative changes, correct typographic errors, adopt consistent terminology, correct grammar, and adopt plain English. These changes are not discussed further.

Note that some of the final rule requirements were relocated. An example is the cyber security requirements that were issued as proposed § 73.55(m) and now reside in § 73.54.

Comments on the three PRMs are not explicitly addressed in the detailed comments response document, beyond those discussed earlier in Section II of this document, as this document addresses only the comments submitted on the proposed rule. However, the petitioner's comments were considered as part of the Commission's decision-making process and final determination of the rule requirements for each of the areas of concern.

Comments on the supporting regulatory analysis of the proposed rule are also contained in the detailed comment response document. Revisions to the final rule regulatory analysis were made consistent with the comment responses and these comments are not addressed further in this section.

The Commission solicited public comment on a number of specific issues but received input on only one of these specific issues. Specifically, the Commission requested stakeholders to provide insights and estimates on the feasibility, costs, and time necessary to implement the proposed rule changes to existing alarm stations, supporting systems, video systems, and cyber security. A commenter stated that the feasibility of establishing a cyber security program for industrial control systems has been demonstrated by various electric utilities, chemical plants, refineries, and other facilities with systems similar, if not identical, to those used in the balance-of-plant in commercial nuclear plants. The commenter stated that the time and cost necessary to implement a cyber security program is dependent on the scope and discussed the technologies and programmatic approaches that can be pursued to augment current industry-proposed generic recommendations. The Commission focused significant attention on the cyber

requirements and supporting guidance during development of the final cyber security requirements in § 73.54 as discussed below.

In general, there was a range of stakeholder views concerning this rulemaking, some supporting the rulemaking, others opposing the rulemaking. Some stakeholders viewed this rulemaking as an effort to codify the insufficient status quo while others described the new requirements as going well beyond the post-September 11, 2001, order requirements. The Commission believes that commenters who suggested that the Commission had no basis to go beyond the requirements that were imposed by the security orders misunderstood the relationship of those orders and the rulemaking. The security orders were issued based on the specific knowledge and threat information available to the Commission at the time the orders were issued. The Commission advised licensees who received those orders that the requirements were interim and that the Commission would eventually undertake a more comprehensive re-evaluation of current safeguards and security programs. As noted in the proposed rule, there were a number of objectives for the rulemaking beyond simply making generically applicable security requirements similar to those that were imposed by Commission orders. The Commission intended to implement several new requirements that resulted from insights it gained from implementation of the security orders, review of site security plans, implementation of the enhanced baseline inspection program, and evaluation of force-on-force exercises. These insights were obviously not available to the Commission when it issued the original security orders in 2002 and 2003.

In addition, another key objective of this rulemaking was to update the regulatory framework in preparation for receiving license applications for new reactors. The current security regulations in part 73 have not been substantially revised for nearly 30 years. Before September 11, 2001, the NRC staff had already undertaken an effort to revise these dated requirements, but that effort was delayed (See SECY-01-0101, June 4, 2001). Thus, this

rulemaking addresses a broader context of security issues than the focus of the security orders of 2002 and 2003. One significant issue in particular was the need for clearly articulated security requirements and a logical regulatory framework for new reactor applicants. The revisions to part 73 were also intended to provide it with needed longevity and predictability for current and future licensees with a measured attempt to anticipate future developments or needs in physical protection.

**B. Section 50.54(hh), Mitigative Strategies and Response Procedures for Potential or Actual Aircraft Attacks.**

As noted previously, a significant change to this final rule is the relocation of and provision of more detailed requirements for the beyond-design basis mitigative measures and potential aircraft attack notification requirements from proposed part 73, appendix C, to 10 CFR 50.54(hh). The Commission received several stakeholder comments that the proposed part 73, appendix C, was not the appropriate location for these requirements. During consideration of these comments, the Commission also decided to add additional detail to the aircraft attack notification portion of the requirements now located in § 50.54(hh)(1). In response, the Commission issued a supplemental proposed rule seeking additional stakeholder comment on these proposed revisions on April 10, 2008, (73 FR 19443) for a 30 day comment period. The Commission received six sets of comments on the supplemental proposed rule. The responses to those comments are discussed as follows.

The Commission revised the final rule language for § 50.54(hh)(1)(ii) in response to comments that the final rule should only require periodic updates to applicable entities or that communications should be maintained “as necessary and as resources allow.” The Commission intended the continuous communication requirement to apply to licensees only with respect to aircraft threat notification sources and not to all offsite response or government organizations. The Federal Aviation Administration (FAA) local, regional, or national offices; North American

Aerospace Defense Command (NORAD); law enforcement organizations; and the NRC Headquarters Operations Center are examples of threat notification sources with which licensees would be required to maintain a continuous communication capability. If a licensee encounters a situation in which multiple threat notification sources (e.g., FAA, NORAD, and NRC Headquarters Operations Center) are providing the same threat information, the licensee would only be required to maintain continuous communication with the NRC Headquarters Operations Center. Because licensees need to be aware when they can cease or must accelerate mitigative actions, it is important that licensees do not lose contact with aircraft threat notification sources. Periodic updates to entities other than threat notification sources are permitted by this final rule.

In response to comments that §§ 50.54(hh)(1)(iii), 50.54(hh)(1)(iv), and 50.54(hh)(1)(vi) requirements were redundant to those found in the NRC's existing emergency preparedness rules, the Commission revised the final rule language for each of those paragraphs to clarify the Agency's intent and to eliminate the appearance of redundant requirements vis-à-vis the emergency preparedness rules, which are also currently being revised. The intent of § 50.54(hh)(1)(iii) is to ensure that licensees contact offsite response organizations as soon as possible after receiving aircraft threat notifications. There is no expectation that licensees will complete and disseminate notification forms as the previous rule text implied. Section 50.54(hh)(1)(iv) pertains to operational actions that licensees can take to mitigate the consequences of an aircraft impact; the Commission did not intend this requirement to include emergency preparedness-related protective actions. In § 50.54(hh)(1)(vi), the Commission intended to require licensees to disperse essential personnel and equipment to pre-identified locations after receiving aircraft threat notifications, but before actual aircraft impacts, when possible. Also, the requirement for licensees to facilitate rapid entry into their protected areas applies only to those onsite personnel and offsite responders who are necessary to mitigate the

event and not to everyone who was initially evacuated from the protected areas.

The Commission revised the statements of consideration for § 50.54(hh)(1)(vi) in response to a comment that meeting the rule might require licensees to suspend security measures under 10 CFR 50.54(x). The Commission elaborated on the specific intent of the protected area evacuation timeline assessment and validation, which is to require licensees to establish a decision-making tool for use by shift operations personnel to assist them in determining the appropriate onsite protective action for site personnel for various warning times and site population conditions. The Commission expects that licensees will incorporate this tool into applicable site procedures to reduce the need to make improvised decisions that would necessitate a suspension of safeguards measures during the pre-event notification period. However, the Commission wishes to make clear that the suspension of security measures to protect the health and safety of security force personnel during emergencies is now governed by § 73.55(p)(1)(ii) as codified in this final rule. Previously, there was no specific provision in the Commission's regulations that would have permitted such a departure, because under § 50.54(x), licensees are only permitted to suspend security measures if the health and safety of the public was at risk. Note that, in a § 50.54(hh) scenario, either §§ 50.54(x) or 73.55(p) could be applicable depending on the circumstances.

The Commission revised the final rule requirements in § 50.54(hh) in response to a comment that the final rule should include an applicability statement that removes the requirements of § 50.54(hh) from reactor facilities currently in decommissioning and for which the certifications required under § 50.82(a)(1) have been submitted. The commenter indicated that it is inappropriate that § 50.54(hh) should apply to a permanently shutdown and defueled reactor where the fuel was removed from the site or moved to an independent spent fuel storage installation (ISFSI). The NRC agrees with this comment and revised the final requirements in § 50.54(hh) so they do not apply to facilities for which certifications have been filed under

§ 50.82(a)(1) or § 52.110(a)(1). The Commission notes that § 50.54(hh) does not apply to any current decommissioning reactor facilities that have already satisfied the § 50.82(a) requirements.

The Commission requested stakeholder feedback on two questions in the supplemental proposed rule. Regarding the first question in the supplemental proposed rule notice where the Commission requested input on whether there should be additional language added to the proposed § 50.54(hh) requirements that would limit the scope of the regulation (i.e., language that would constrain the requirements to a subset of beyond-design basis events such as beyond-design basis security events), commenters indicated that the Commission should constrain the requirements to a subset of beyond-design basis events; namely beyond design basis security events. The feedback suggested that, by limiting the rule requirements to strategies that address a generic set of beyond-design basis security events, the strategies could then be developed and proceduralized to focus on the restoration capabilities needed to mitigate the effects from these events. After careful consideration, the Commission decided to maintain the language from the supplemental proposed rule that recognizes that the mitigative strategies can address losses of large areas of a plant and the related losses of plant equipment from a variety of causes including aircraft impacts and beyond-design basis security events. The Commission also requested comments on whether applicants should include, as part of a combined license or operating license application, the § 50.54(hh) procedures, guidance, and strategies. Commenters indicated that this information will not be needed until fuel load, when an aircraft threat would be present. The most appropriate and efficient process for the Commission is to review these procedures as part of the review of operations procedures and beyond-design basis guidelines. The Commission views the mitigative strategies as similar to those operational programs for which a description of the program is provided and reviewed by the Commission as part of the combined license application and subsequently the more detailed

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

**C. Section 73.2, Definitions.**

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

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

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

authorization program required by § 73.56; the cyber security plan is subject to the same licensing requirements as the licensee's physical security, training and qualification, and safeguards contingency plans. In relocating these requirements, the Commission concluded that certain administrative requirements, otherwise applied by inclusion in § 73.55, must be brought forward for consistency. As a result, conforming changes were made to the pre-existing §§ 50.34(c) and 50.34(e) to establish the appropriate regulatory framework for Commission review and approval of the cyber security plan required by § 73.54(e). These conforming changes require nuclear power reactor applicants to provide a cyber security plan as part of the security plans currently required by §§ 50.34(c) or 52.79(a)(36), as applicable. Additionally, conforming changes were made to § 50.54(p), applicable to both operating and combined licensees, to require a cyber security plan as a condition of the license. Conforming changes were also made to §§ 50.34(e) and 52.79(a)(36) to require applicants to review this plan against the criteria for Safeguards Information established in § 73.21. Consistent with § 73.54(b)(3), the cyber security program is a part of the physical protection program subject to the same review and approval mechanisms as the physical security plan, training and qualification plan, and safeguards contingency plan.

The Commission has also added three (3) administrative requirements to the final rule (§§ 73.54(f), 73.54(g), and 73.54(h)) to require written policies and procedures, program review, and records retention, respectively.

In addition to the previously mentioned conforming changes, the Commission added an undesignated paragraph at the beginning of this section to require current licensees subject to § 73.54 to submit a cyber security plan and implementation schedule for Commission review and approval. The licensee's cyber security plan must be submitted by way of a license amendment pursuant to 10 CFR 50.90.

Section 73.54(a), Protection. The Commission received a comment suggesting that the

term “emergency preparedness,” as it appears in the proposed § 73.55(m)(1), should be replaced with the term “emergency response.” In the final rule, the term “emergency preparedness” is replaced with the more generic term “emergency preparedness functions.” The equipment embodied within these preparedness functions as described in 10 CFR part 50, appendix E, usually includes a wide variety of plant monitoring systems, protection systems, and the onsite and offsite emergency communications systems used during an emergency event.

The term “emergency response” suggested by the commenter is used more specifically to refer only to the "emergency response data system" or ERDS, which provides a data link that transmits key plant parameters. Therefore, using the term "emergency preparedness functions" is considered the most appropriate term as it holistically addresses the equipment used during an emergency.

The Commission revised the proposed § 73.55(m)(1) which is renumbered in the final rule as § 73.54(a). This paragraph has been expanded to provide a more detailed list of the types of systems and networks that are intended to be included consistent with the proposed rule. The language in § 73.54(a)(1)(ii) is revised to clarify that "digital computer and communications systems and networks" must be considered for protection. It is important to note that the Commission does *not* intend that CAS or SAS operators be responsible for cyber security detection and response but rather that this function will be performed by technically trained and qualified personnel.

<u>Section 73.54(b), Analysis of Digital Computer and Communication Systems and Networks</u>. The requirement to document a site-specific analysis that identifies site-specific conditions has been brought forward from § 73.55(b)(4). The rule is clarified to require that each licensee analyze the digital computer and communication systems and networks in use at their facility to identify those assets that require protection against the design basis threat.

The proposed § 73.55(m)(1) requirement to establish, implement, and maintain a cyber

security program is renumbered in the final rule as § 73.54(b)(2). The rule requires that the cyber security program will include measures for the adequate protection of the digital computer and communication systems and networks identified by the licensee through the required site-specific analysis stated in § 73.54(b)(1).

The proposed § 73.55(m)(1)(ii) is renumbered in the final rule as § 73.54(b)(3). The Commission received several comments that the cyber security program is not appropriate for incorporation into the physical security program and, therefore, should not be implemented through the security organization. The Commission agrees in part. Cyber security, like physical security, focuses on the protection of equipment and systems against attacks by those individuals or organizations that would seek to cause harm, damage, or adversely affect the functions performed by such systems and networks. Cyber security and physical security programs are intrinsically linked and must be integrated to satisfy the physical protection program design criteria of §73.55(b). The Commission recognizes that a uniquely independent technical expertise and knowledge is required to implement the cyber security program effectively, and therefore, the specific training and qualification requirements for the program must focus on ensuring that the personnel are trained, qualified, and equipped to perform their unique duties and responsibilities.

Section 73.54(c), Cyber Security Program. The proposed §73.55(m)(1)(iii) is renumbered in the final rule as §73.54(c) and (c)(1), and is revised to clarify appropriate design requirements for the cyber security program. The cyber security program must be designed to implement security controls to protect the digital assets identified by the paragraph (b)(1) analysis. To accomplish this, the final rule §73.54(c)(2), (3), and (4) are added to clarify the performance criteria to be met through implementation of the cyber security program.

The Commission received a comment that the term "protected computer system" in the proposed §73.55(m)(1)(iii) is not defined and urged a more specific description. The

Commission has deleted the term “protected computer system” from the final rule and provided a more detailed description of digital computer and communication systems and networks in §73.54(a)(1).

The Commission received a comment that the high assurance requirement of the proposed § 73.55(m)(1) does not allow a licensee to implement measures designed to ensure continued functionality. Section 73.54(c)(4) has been revised to require the cyber security program to be designed to ensure that the intended function of the assets identified by §73.54(b)(1) are maintained.

The proposed § 73.55(m)(5) is renumbered in the final rule as § 73.54(c)(2). The Commission received a comment to the proposed § 73.55(m)(5) that questioned whether the phrase “defense-in-depth” in computer terminology was intended to include real-time backup data. The Commission concluded that defense-in-depth for digital computer and communication systems and networks includes technical and administrative controls that are integrated and used to mitigate threats from identified risks. The need to back-up data as part of a defense-in-depth program is dependent upon the nature of the data relative to its use within the facility or system.

Defense-in-depth is achieved when (1) a layered defensive model exists that allows for detection and containment of non-authorized activities occurring within each layer, (2) each defensive layer is protected from adjacent layers, (3) protection mechanisms used for isolation between layers employ diverse technologies to mitigate common cause failures, (4) the design and configuration of the security architecture and associated countermeasures creates the capability to sufficiently delay the advance of an adversary in order for preplanned response actions to occur, (5) no single points of failure exist within the security strategy or design that would render the entire security solution invalid or ineffective, and (6) effective disaster recovery capabilities exist for protected assets.

The commenter also questioned how this requirement impacts the video image recording system, which is a computer system required by § 73.55(e)(7)(i)(C) . Based upon the licensee's site-specific analysis, the video image recording system may be subject to this requirement if it meets the criteria stipulated in § 73.54(a)(2), but it is not required to be included by the final rule.

Section 73.54(d), Cyber-Related Training, Risk, and Modification Management. The Commission has consolidated the proposed requirements from §§ 73.55(m)(2), (m)(6), and (m)(7) into one paragraph of the § 73.54(d) to require the development, implementation, and maintenance of supporting programs within the cyber security program. The Commission has moved proposed § 73.54(m)(6) to § 73.54(d)(3) and clarified it to require that an evaluation be performed prior to modifications to protected digital assets to ensure that the cyber performance objectives of § 73.54 are maintained.

The Commission received a comment to the proposed rule § 73.55(m)(2) requesting clarification of what is meant by "assessment." The term "assessment" has been removed from the final rule. To ensure that the measures used to protect digital computer and communication systems and networks remain effective and continue to meet high assurance expectations, the cyber security program must evaluate and manage cyber risks. Licensees must evaluate changes to systems and networks when (1) modifications are proposed for previously analyzed systems and (2) new technology-related vulnerabilities, not previously analyzed in the original analysis, that would act to reduce the cyber security environment of the system are identified.

Section 73.54(e), Cyber Security Plan. The proposed § 73.55(m)(1)(i) is renumbered in the final rule as § 73.54(e). The Commission added a new § 73.54(e)(1) generically addressing the content of the cyber security plan. The plan must describe and account for any site-specific conditions that affect how Commission requirements are implemented.

The proposed § 73.55(m)(4)(ii) is deleted from the final rule. Consistent with the removal of this section from the proposed § 73.55(m), the Commission concluded that it is appropriate to

address the cyber security incident response and recovery plan in the cyber security plan required by this section. The rule requires that the cyber security incident response and recovery plan will be part of the cyber security plan which in turn will be a component of the physical security program.

The proposed §§ 73.55(m)(4)(i) and (m)(4)(iii) are combined and renumbered to the final rule § 73.54(e)(2). The Commission received a comment to the proposed § 73.54(m)(4)(i) that there should be a rule requirement prescribing the timeframe in which a licensee must determine that a cyber attack is occurring or has occurred and suggested that it be within minutes of the attack. The Commission agrees with the commenter's concerns. The proposed § 3.54(m)(4)(iii) is renumbered in the final rule as § 73.54(e)(2)(i) and is revised to require a description in the cyber plan of how the licensee will maintain the capability for timely detection and response to cyber attacks. Licensees are required to develop, implement, and maintain a methodology for detecting cyber attacks; however, they are not required to meet deterministic time limits for discovery of a cyber attack. The cyber security program must be designed to ensure that cyber attacks are detected and an appropriate response is initiated to prevent the attack from adversely affecting the systems and networks that must be protected. The Commission has concluded that the § 73.54 performance-criteria and requirements ensure that detection and response are appropriate.

Section 73.54(f), Policies and Procedures. The proposed § 73.55(m)(3) is renumbered in the final rule as § 73.54(f). The Commission added § 73.54(f) to clarify that policies, implementing procedures, site-specific analysis, and other supporting technical information used by the licensee need not be submitted for Commission review and approval as part of the cyber security plan. However, this information must be made available upon request by an authorized representative of the Commission.

Section 73.54(g), Reviews. The Commission added the final rule § 73.54(g). The

requirement for the review of the cyber security program is subject to the same processes stipulated in § 73.55(m), "Security program reviews."

Section 73.54(h), Records. The Commission added the final rule § 73.54(h). Consistent with establishing § 73.54 as a stand-alone 10 CFR section, this requirement for the retention of the cyber security program records is brought forward from the final rule § 73.55(q), "Records." The expectation is that each licensee will maintain the technical information associated with the assets identified by the final rule § 73.54(b)(1) that is pertinent to compliance with § 73.54.

**E. Section 73.55 Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage.**

General Comments. The Commission received several general comments which stated that the proposed § 73.55 does not include requirements for protection against aircraft attacks. As the Commission recently stated in the final design basis threat rulemaking (72 FR 12705; March 19, 2007), the protection of NRC-regulated facilities against aircraft attacks is beyond the scope of a licensee's obligations. Accordingly, requiring specific measures for the protection against aircraft attacks is beyond the scope of the requirements presented in this section and, therefore, is not addressed. The Commission nevertheless notes that there are requirements in this rulemaking that address licensee actions that are required to minimize the potential consequences of an aircraft impact on a nuclear power plant. As noted previously, those requirements are now located in § 50.54(hh) as conditions of license.

Section 73.55(a), Introduction. The proposed § 73.55(a) would have required each licensee to submit, in their entirety, a revised physical security plan, training and qualification plan, and safeguards contingency plan for NRC review and approval within 180 days after the effective date of the final rule. The Commission received several comments stating that 180 days is not sufficient time to review and understand the modifications that may be required for compliance with the amended rule and to revise and submit amended security plans. In

response to the comments, the Commission determined that, with the exception of the cyber security plan required by the new § 73.54, the majority of plan changes needed for compliance with the amended requirements of this section are likely to be minimal and are not anticipated to decrease the effectiveness of any particular licensee's current security plan. Because the current NRC-approved security plans already address the Commission's orders and pre-existing 10 CFR requirements, the greatest impact of this final rule will be focused primarily on those changes to plans and procedures needed to satisfy the requirements that are identified as "new." The rule requires that within 180 days of the effective date of the rule, each currently operating reactor licensee must evaluate, on a site-specific basis, what security plan changes are needed to comply with the amended requirements of the rule. Those changes must be incorporated into their security plans, as necessary, within the same 180 days. In doing so, licensees are expected to follow the appropriate change processes described currently in §§ 50.54(p), 50.90, or 73.5. The Commission acknowledges that based on site-specific conditions, a limited number of plan changes may require Commission review and approval before implementation and must be made through a license amendment pursuant to 10 CFR § 50.90 or a request for an exemption per 10 CFR 73.5.

The Commission deleted the proposed requirements in § 73.55(a)(2) and (a)(3) for consistency with the determination that revised plans need not be submitted to the Commission for review and approval.

The Commission added a requirement in § 73.55(a)(2) that licensees must identify, describe, and account for site-specific conditions that affect the licensee's ability to satisfy the requirements of this section in the NRC-approved security plans. This requirement is added for consistency with revisions made to § 73.55(b)(4) which requires each licensee to conduct a site-specific analysis to identify such conditions.

The proposed § 73.55(a)(4) is renumbered in the final rule as § 73.55(a)(3) with minor

revision to delete reference to Commission orders. One commenter asked the NRC to clarify its position with respect to the "legally-controlling document" once it approves a licensee security plan. Once a licensee has an approved security plan, both the licensee's security plan and the Commission's regulations are legally controlling. Regulations are legally controlling to the extent that they set forth the regulatory framework and general performance objectives of a licensee's security plan. The NRC-approved security plan, in contrast, describes a licensee's method of complying with those regulations including exemptions and approved alternatives. However, that the NRC specifically approved a licensee's security plan does not relieve the licensee from compliance with regulations.

To the extent that there are differences in a licensee's security plan and the regulatory requirements, the Commission expects that those differences would be specifically approved by the NRC, either in the form of an NRC-granted exemption, or an NRC-approved "alternative measure" as set forth in § 73.55(r). The NRC recognizes that generic regulations cannot always account for site-specific conditions. Some degree of regulatory flexibility is necessary to ensure that each licensee is capable of meeting the general performance objective of § 73.55(b)(1) to provide "high assurance" of public health and safety and common defense and security despite site specific conditions or situations that may interfere with or prevent the effective implementation of a given NRC requirement. Therefore, these regulations provide several mechanisms through which the NRC may approve a licensee's plan to implement alternative measures or exempt a licensee from compliance with any one or more NRC requirements, provided the licensee documents and submits sufficient justification. Once those exemptions or alternative measures are specifically reviewed and approved by the NRC and are incorporated into the licensee's security plan, they then become legally binding through the licensee's security plan required as a condition of its license.

In the rare situation in which a licensee's security plan conflicts with NRC regulations and

the NRC has not reviewed and approved the conflicting measures, the Commission expects that the staff would work with the licensee to ensure that the security plan is revised to comply with the regulatory requirement. That the security plan may have been approved with a deficiency does not excuse the licensee from compliance with the Commission's regulations.

Section 73.55(a)(4) establishes when an applicant's physical protection program must be implemented. The Commission concluded that the receipt of special nuclear material (SNM) in the form of fuel assemblies onsite, i.e. in the licensee's protected area, is the event that subjects a licensee to the requirements of § 73.55. It is the responsibility of the applicant/licensee to implement an effective physical protection program before SNM in the form of fuel assemblies is received in the protected area.

The Commission has added a new requirement in § 73.55(a)(5) to address the Tennessee Valley Authority (TVA) facility at Watts Bar. TVA is in possession of a current construction permit for Watts Bar Nuclear Plant, Unit 2, and is treated as a current licensee for purposes of satisfying the requirements of this rule. These requirements reflect Commission support of a licensing review approach for Watts Bar Nuclear Plant, Unit 2, that employs the current licensing basis for Unit 1 as the reference basis for review and licensing of Unit 2, as stated in a July 25, 2007, Staff Requirements Memorandum (ML072060688).

The Commission has revised the final rule § 73.55(a)(6) to clarify that certain requirements in this section apply only to applicants for an operating license under the provisions of 10 CFR part 50 of this chapter, or holders of a combined license under the provisions of 10 CFR part 52 of this chapter. Specifically, the requirements to design, construct, and equip both the CAS and SAS to the same standards are addressed in the final rule as § 73.55(i)(4)(iii). The Commission views this as a prudent safety enhancement for future nuclear power plants but not an enhancement that is necessary for the adequate protection of pre-existing operating reactors. Unless otherwise specifically approved by the Commission, pre-

existing power reactor licensees choosing to construct a new reactor inside an existing protected area are subject to the new CAS/SAS requirements in § 73.55(i)(4)(iii).

Section 73.55(b), General Performance Objective and Requirements. The Commission received several comments requesting that the term "radiological sabotage" be used in lieu of the phrase "significant core damage" and "spent fuel sabotage" because the term "radiological sabotage" is defined in § 73.2. The Commission agrees in part and has revised the final rule in § 73.55(b)(2) to clearly retain, without modification, the pre-existing requirement for licensees to provide protection against the design basis threat of radiological sabotage and has revised § 73.55(b)(3) to clarify that the design of the physical protection program must ensure the capability to prevent "significant core damage" and "spent fuel sabotage." It was not the Commission's intent in the proposed rule to delete the requirement for protection against radiological sabotage but rather to establish the prevention of significant core damage and spent fuel sabotage as the criteria to measure a licensee's performance to protect against "radiological sabotage." The final rule has been revised to reflect this intent. The achievement of "significant core damage" and "spent fuel sabotage" can be measured by the licensee through accepted engineering standards, and the use of these terms provides measurable performance criteria that are essential to understanding the definition of radiological sabotage. Additionally, the Commission believes that continued use of the terms "significant core damage" and "spent fuel sabotage" to enhance the understanding of radiological sabotage is warranted because these terms are now well established and have been used consistently by the Commission and industry relative to force-on-force testing before and after September 11, 2001.

The Commission received several comments regarding the proposed rule § 73.55(b)(2), the introduction of six performance-criteria: detect, assess, intercept, challenge, delay, and neutralize. Upon consideration, the Commission concluded that the four terms, "detect, assess, interdict, and neutralize," more concisely represent the intended performance-criteria and this

change has been made throughout the final rule. The terms “intercept, challenge, and delay” are subsumed in the term “interdict.”

The Commission received a comment that the proposed rule § 73.55(b)(3) delineation of requirements for the design of the physical protection program should be clarified. The Commission agrees and § 73.55(b)(3) has been revised to clarify Commission expectations. The requirement for the protection of personnel, equipment, and systems against the design basis threat vehicle bomb assault is addressed in the § 73.55(e)(10)(i)(A). The requirement for protection against a single act, within the capabilities of the design basis threat of radiological sabotage, is based upon the pre-existing § 73.55(e) and is addressed in the final rule § 73.55(i)(4)(i). Section 73.55(i)(4)(i) requires licensees to protect either the CAS or SAS against a single act by ensuring the survival of at least one alarm station in order to maintain the ability to perform required functions.

Section 73.55(b)(4) is renumbered in the final rule as § 73.55(b)(3)(ii). The Commission received a comment that the scope of the proposed § 73.55(b)(4) regarding the term “defense-in-depth” was not clearly understood. Section 73.55(b)(3)(ii) is revised to clarify that defense-in-depth is accomplished through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure the overall effectiveness of the physical protection program.

Section 73.55(b)(4) is added to specifically require that each licensee perform a site-specific analysis for the purpose of identifying and analyzing site-specific conditions that affect the design of the onsite physical protection program. Commission regulations are generic and cannot in all instances account for site-specific conditions, and therefore, it is the licensee’s responsibility to identify and account for site-specific conditions relative to meeting Commission requirements, subject to NRC inspection.

Section 73.55(b)(8) is added to require the development and maintenance of a cyber

security program that meets the performance objectives of the new § 73.54. Section 73.54 incorporates the proposed § 73.55(m) in its entirety, and the associated public comments were addressed previously within the new § 73.54.

Section 73.55(b)(10) is revised to clarify the Commission's expectation that each licensee will enter physical protection program findings and deficiencies into the site corrective action program so that they can be tracked, trended, corrected, and prevented from recurring.

Section 73.55(b)(11) is repeated from the pre-existing appendix C to part 73, "Introduction," to delineate the Commission's expectation that security plans and implementing procedures must be complementary to other site plans and procedures.

Section 73.55(c), Security Plans. The Commission received several comments stating that the requirements in § 73.55(c) are redundant to the requirements in § 50.34(c) and (d). The Commission disagrees. While these requirements appear to be redundant, conforming changes have been made to § 50.34(c) and (e) to include cyber security plans and training and qualification plans. In addition, § 73.55 establishes a paragraph dedicated to security plans to consolidate the regulatory framework for each plan, describe the general content of each plan, and clarify the relationship between Commission regulations, NRC-approved security plans, and site-specific implementing procedures. The primary focus of the security plans is to describe how the licensee will satisfy Commission requirements including how site-specific conditions affect the measures needed at each site to ensure that the physical protection program is effective.

The Commission received a comment that the proposed § 73.55(c)(2) appeared to require that all security plans be protected as Safeguards Information (SGI). The Commission disagrees with the comment. Licensees are required by § 73.55(c)(2) only to review the information contained in the security plans against the criteria contained in § 73.21 to determine the existence of SGI and to protect that information appropriately.

The Commission has added a conforming requirement to §§ 73.55(c)(6) and 50.34(c) for licensees to provide a cyber security plan in accordance with the new § 73.54 for Commission review and approval.

The proposed §§ 73.55(c)(3)(ii), 73.55(c)(4)(ii), and 73.55(c)(5)(ii) are deleted from the final rule. The Commission's expectation is that each licensee will address Commission requirements in their approved plans and implementing procedures and, where the Commission requires a specific detail to be included in the plans, that requirement is stated in applicable paragraphs of the final rule.

Section 73.55(d), Security Organization. The Commission received several comments that the proposed requirement of § 73.55(d)(1) to provide "early detection, assessment, and response to unauthorized activities within any area of the facility" was too broad and could result in unnecessary regulatory burden. The Commission agrees with the comment and has deleted these terms and revised the language to clarify the primary responsibility of the security organization. The intent is that the security organization will focus upon the effective implementation of the physical protection program which in turn is designed to protect the facility from the design basis threat of radiological sabotage with high assurance.

The Commission received a comment that proposed § 73.55(d)(3) was not clearly understood as it appeared this requirement may pertain to any individual within the security organization. The Commission agrees, and the final rule text in § 73.55(d)(3) is revised to clarify that individuals assigned to perform physical protection and/or contingency response duties must be trained, equipped, and qualified in accordance with appendix B to part 73 to perform those assigned duties and responsibilities whether that individual is a member of the security organization or not. This clarification is made to account for those instances where the licensee uses facility personnel other than members of the security organization to perform duties within the physical protection program, such as a vehicle escort or warehouse personnel inspecting/

searching deliveries. The rule requires that facility personnel who are not members of the security organization will be trained and qualified for the specific physical protection duties that they are assigned, which includes possessing the knowledge, skills, abilities, and the minimum physical qualifications such as sight, hearing, and the general health needed to perform the assigned duties effectively.

The proposed § 73.55(d)(4) is deleted from the final rule because the reference to meeting the requirements of § 73.56 (Access authorization program) is redundant.

The Commission received several comments indicating that the requirements in the proposed § 73.55(d)(5) pertaining to contracted security forces were redundant to other requirements addressed in the proposed rule. The Commission agrees. These requirements were retained from pre-existing requirements for the licensee to explicitly include these requirements as written statements in contracts between the licensee and a contract security force. Upon review, the Commission has determined that specifying these requirements in written contracts is unnecessary. The enforceability of NRC regulatory requirements is not dependent on whether they are implemented by the licensee or by a licensee contractor; therefore, specifically requiring the contract between these parties to contain these requirements is unnecessary. The Commission has, however, retained the requirement in the final rule § 73.55(q)(3), "Records," (formally described in proposed § 73.55(d)(5)) that a copy of the contract be retained by the licensee. Additionally, the requirement in the proposed § 73.55(d)(5)(vi) that "any license for possession and ownership of enhanced weapons will reside with the licensee" has been deleted from this section. The Commission intends, however, that this requirement will be reflected in its regulations codifying requirements related to the use of enhanced weapons. The Commission's plan for that rulemaking was stated previously in this document. The remaining proposed requirements of § 73.55(d)(5) are deleted from this paragraph and are retained in other paragraphs of the final rule.

Section 73.55(e), Physical Barriers. The Commission received several comments that the proposed § 73.55(e) would result in unnecessary regulatory burden by expanding protected area physical barrier requirements into the owner controlled area (OCA). The Commission agrees in part and § 73.55(e) is revised to clarify the generic and specific requirements for the design, construction, placement, and function of each physical barrier. Section 73.55(e)(6) specifically addresses requirements for physical barriers in the OCA. Physical barriers can be used to fulfill many functions within the physical protection program, and therefore, each physical barrier must be designed and constructed to serve its predetermined function within the physical protection program. Consistent with § 73.55(b) for design of the physical protection program, the rule requires that each licensee will analyze site-specific conditions to determine the specific use, type, function, construction, and placement of physical barriers needed for the implementation of the physical protection program.

The Commission received comments on the proposed § 73.55(e)(3)(i), which would have required the delineation of the boundaries of areas for which the physical barrier provides protection, requesting that this provision be deleted because it lacked performance criteria. The Commission agrees, and the requirement is deleted from the final rule because it is more appropriate to be specified in regulatory guidance.

The proposed § 73.55(e)(3)(ii) is renumbered in the final rule as § 73.55(e)(3)(i) and is broken into subparagraphs § 73.55(e)(3)(i)(A) through (C). The Commission received a comment to clarify the proposed rule statements of consideration pertaining to the performance criteria for physical barriers. The Commission agrees in part. The pre-existing § 73.55(c)(8) introduced design goals relative to the use of vehicle barriers but did not address other physical barriers. The statements of consideration in the proposed rule attempted to incorporate other physical barriers and explain that the generic performance-criteria for physical barriers are not limited to vehicle barriers. The criterion for physical barriers is that "*each barrier be designed to*

*satisfy the function it is intended to perform.*" The Commission agrees with the comment stating that the performance of all three functions (i.e., visual deterrence, delay, and support access control measures) is not always required of each barrier, and the final rule addresses the barrier design requirements generically in § 73.55(e)(3)(i)(A) through (C).

The Commission received several comments requesting clarification of the proposed rule § 73.55(e)(4) for physical protection measures in the OCA. The proposed § 73.55(e) attempted to establish a generic requirement for the design, construction, placement, and function of physical barriers based on a site specific analysis. This generic requirement was misunderstood to mean that PA barriers were now required in the OCA. As such, the Commission revised the proposed § 73.55(e) and (e)(6) to clarify the scope and intent of this requirement. Consistent with the final rule § 73.55(b)(4), it is the responsibility of each licensee to identify, analyze, and account for site-specific conditions in the design and implementation of its physical protection program. Section 73.55(e)(6) is revised to clarify that the application of physical barriers in the OCA is determined by each licensee through site-specific analysis and must satisfy the physical protection program design requirements of § 73.55(b). The rule requires that the licensee will design and construct appropriate barriers in those areas to meet the identified site-specific need.

The Commission received comments requesting clarification of the term "unobstructed observation" as used in § 73.55 (e)(5)(i)(A). The Commission agrees that this term can be misunderstood, and therefore, § 73.55(e)(7)(i)(A) is revised to delete the term "unobstructed." This term was used to emphasize that a clear field of observation be provided in the isolation zone. However, the Commission's expectation is not the complete elimination of obstruction but that the licensee implement measures needed to negate the effects of any obstructions such as the relocation of non-permanent objects or the strategic placement of cameras to enable observation around an obstruction.

The Commission received several comments to clarify the proposed § 73.55(e)(5)(ii)

pertaining to the performance of isolation zone assessment equipment and agrees that clarification is necessary. The proposed § 73.55(e)(5)(ii) is renumbered in the final rule as § 73.55(e)(7)(i)(C) and provides a performance-based description for specific isolation zone assessment equipment. The Commission has concluded that the requirement for this equipment is consistent with current licensee practices, therefore, it is an appropriate update for this final rule.

The proposed § 73.55(e)(5)(iii) is renumbered in the final rule as § 73.55(e)(7)(ii). The Commission received a comment that this requirement would preclude the use of areas inside the protected area as equipment lay-down/staging areas. The Commission agrees in part. The final rule does not preclude the use of lay-down areas/staging areas. However, this requirement does explicitly preclude such activities where the action constitutes an obstruction that prevents observation on either side of the protected area perimeter. This rule requires the licensee to take appropriate actions to negate any adverse effects that lay-down/staging areas may have to prevent observation on either side of the protected area perimeter.

The Commission received several comments to clarify the proposed requirement in § 73.55(e)(6)(i) to secure penetrations through the protected area barrier. The Commission agrees that clarification is necessary. The proposed requirement is separated and renumbered as § 73.55(e)(8)(ii). Section 73.55(e)(8)(ii) is revised to clarify that penetrations must be secured and monitored to prevent exploitation. Where the size of an opening in any barrier is large enough to be exploited or otherwise defeat the intended function of that barrier, then such openings must be secured and monitored to prevent or detect attempted or actual exploitation.

The proposed § 73.55(e)(6)(v) is renumbered to § 73.55(e)(5). The Commission received several comments to clarify the term “bullet-resisting.” The Commission agrees in part that additional clarification is needed but does not believe that such clarification is necessary in the rule text. The Commission has determined that it is not appropriate to publicly reference site

specific bullet-resisting standards in the rule because such specificity may lead to the identification of specific vulnerabilities. Specific bullet resisting standards that meet the requirements in § 73.55(e)(5) are described in regulatory guidance and would be further reflected in a licensee's NRC-approved security plans. The Commission acknowledges, however, that in addition to manufactured bullet-resisting materials, a level of bullet-resistance that meets the intent of this regulation might be provided by distances and angles combined with standard construction materials and designs.

The proposed § 73.55(e)(6)(vi) is renumbered in the final rule as § 73.55(e)(8)(v). The Commission received several comments requesting that the NRC delete the word "all" with respect to its modification of the term "exterior areas." The Commission agrees that clarification is necessary. Section 73.55(e)(8)(v) retains and updates the pre-existing requirement in § 73.55(c)(4) to periodically check *all* exterior areas within the protected area but has revised the requirement to clarify that some areas may be excepted from this requirement where safety concerns prevent the licensee from physically checking that area. The Commission's expectation is that licensee procedures will account for these areas by another means that ensures the safety of personnel while assuring the integrity of the area and the requirement is met.

Section § 73.55(e)(9)(v)(D) is added to include the SAS among the types of areas and equipment that must be afforded protection as a vital area/equipment the same as the CAS, only for *applicants* for new reactor licenses. Current licensees are not subject to this requirement as they have been found to provide adequate protection within current configurations. The requirement to treat SAS as a vital area is an enhancement that provides equivalency and redundancy for the alarm stations.

The Commission received a comment that proposed § 73.55(e)(7)(iii), renumbered to the final rule as § 73.55(e)(9)(vi)(A), expands the requirement for secondary power systems from

just “alarm annunciator equipment” to all “intrusion detection and assessment equipment” and that this is a significant expansion that is not explained or supported by NRC force-on-force inspections. The Commission agrees that the scope of the proposed paragraph appears to have been expanded to require all intrusion detection and assessment equipment employed by the licensee to be connected to a secondary power supply and for all secondary power supplies to be treated as vital areas. Section 73.55(e)(9)(vi)(A) is revised to retain the pre-existing § 73.55(e)(1) to locate the secondary power supply for alarm annunciation equipment in a vital area. The Commission has added § 73.55(i)(3)(vii) to address uninterruptible power supplies for intrusion detection and assessment equipment at the protected area perimeter. The uninterruptible power supply discussed in § 73.55(i)(3)(vii) is not required to be located in a vital area because it is a short-term measure utilized to provide service until secondary power sources are operable and the Commission recognizes that uninterruptible power supplies are physically dispersed across the site. Making each uninterruptable power supply a vital area is considered a safety enhancement and implementation would be an unnecessary regulatory burden on the licensee based on the level of protection that would be provided versus the cost.

The Commission has determined that the proposed § 73.55(e)(7)(iv) was redundant to § 73.58 and has deleted this requirement from final rule to avoid unintended duplication and impact beyond current requirements.

The Commission received multiple comments stating that the proposed § 73.55(e)(8) significantly expands the requirements for controlling vehicles inside the OCA. The pre-existing § 73.55(c)(7) requires the licensee to provide vehicle control measures, including vehicle barrier systems, to protect against use of a land vehicle as a means of transportation to gain unauthorized proximity to vital areas. The Commission’s intent is not to expand the requirements for controlling vehicles in the OCA and has revised and consolidated the proposed rule § 73.55(e)(8) to clarify scope and intent of this requirement. The proposed § 73.55(e)(8) is

renumbered in the final rule as § 73.55(e)(10) and provides general vehicle control requirements. In addition, the rule requires that licensees implement security measures to prevent unauthorized access to the protected area by rail.

The Commission received several comments on proposed § 73.55(e)(8)(ii) that to control vehicle approach routes is broader in scope than protecting against vehicle bomb attacks and preventing vehicle use as a means of adversary transportation as was stated in the proposed rule. In lieu of a specific requirement to control vehicle approach routes, § 73.55(e)(10) provides general vehicle control requirements. The Commission acknowledges that the control of vehicle approach routes is generally accomplished through the establishment of vehicle control measures such as a vehicle barrier system designed for protection against vehicle bomb assaults or a protected area barrier that prevents unauthorized personnel from gaining proximity to protected areas or vital areas.

The proposed § 73.55(e)(8)(iii) is modified and renumbered as § 73.55(e)(10)(i)(A). The Commission received several comments to clarify protection requirements against land vehicle bombs and the protection of personnel, systems, and equipment. The Commission agrees, and § 73.55(e)(10)(i)(A) is revised to clarify the protection of personnel, systems, and equipment relative to land vehicle bomb assaults rather than the design basis threat in its entirety. This requirement does not include an obligation to protect all plant personnel from such an attack but rather focuses on the protection of those personnel whose job functions make them necessary to prevent significant core damage and spent fuel sabotage through the implementation of the protective strategy.

The proposed § 73.55(e)(8)(v) is renumbered as § 73.55(e)(10)(i)(B). The Commission received a comment to clarify whether loss of power testing is subject to this requirement. The Commission concluded that specific testing criteria and periodicity are site-specific and must be addressed in procedures. The rule requires that each licensee will develop and implement

procedures that will ensure that active vehicle barriers can be electronically, manually, or mechanically placed in the denial position to perform their intended function for protection against the vehicle bomb in the event of a power failure.

The proposed § 73.55(e)(8)(vi) is renumbered as § 73.55(e)(10)(i)(C). The Commission received several comments that if the proposed § 73.55(e)(8)(vi) is intended to address tampering then the term “tampering” should be used. The Commission agrees and § 73.55(e)(10)(i)(C) is revised to remove the term “integrity,” and clarified to require that the licensee implement measures to identify indications of tampering with vehicle barriers and barrier systems and to ensure that barriers are not degraded. The rule requires that the licensee will implement appropriate surveillance and observation measures for vehicle barriers, barrier systems, and railway barriers.

Section 73.55(e)(10)(i)(D) was specifically added, based on a comment, to address vehicle control measures for sites that have rail access to the protected area.

Section 73.55(e)(11)(iii)(C) is revised to require licensees to provide periodic surveillance and observation of waterway approaches and adjacent areas. Section 73.55(e)(11) is also revised to delete reference to early detection, assessment, and response, consistent with revisions made to the proposed § 73.55(d)(1).

The proposed § 73.55(e)(10) is deleted. The Commission received several comments that this provision is inconsistent with the existing regulations and associated regulatory guidance for openings in the protected or vital areas. The Commission agrees and furthermore determined that “Unattended Openings” are adequately addressed in regulatory guidance and, therefore, need only be addressed through a more generic requirement within this rulemaking. Section 73.55(e)(8)(ii) and § 73.55(i)(5)(iii) generically address penetrations through the PA barrier and unattended openings that intersect a security boundary. The rule requires that such penetrations and unattended openings will be secured and monitored consistent with the

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

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

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

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

attacks on target sets is not appropriate. The Commission disagrees, concluding that § 73.55(f)(2) is appropriate and consistent with Commission requirements for protection against the design basis threat of radiological sabotage stated in § 73.1 and the cyber security requirements stated in the new § 73.54.

The Commission received a comment that the proposed § 73.55(f)(3) requirement to list target set equipment or elements that are not within a protected or vital area in the approved security plan is an unnecessary regulatory burden that could require plan changes whenever site-conditions change. The Commission agrees that targets sets must be adjusted consistent with changes to site-specific conditions, and therefore, § 73.55(f)(3) is revised to require that target set elements not contained in a protected or vital area be identified through the documentation required in § 73.55(f)(1) rather than security plans to ensure that they can be appropriately updated and modified to account for changes to site-specific conditions without prior Commission approval.

The Commission received comments that the proposed § 73.55(f)(4), which would have required implementation of a program to ensure that changes to the configuration of equipment that was identified as target set equipment in the licensee's security plan, was not appropriate due to the increased burden of oversight identified by the requirement. The Commission agrees in part. Section 73.55(f)(4) is revised to clarify the Commission's expectation that each licensee implement a process for the oversight of target set equipment, systems, and configurations using existing processes. This requirement ensures that changes made to the configuration of target set equipment and modes of operation are considered in the licensee's protective strategy. Reference to "significant core damage and spent fuel sabotage" is deleted to clarify that the focus of this requirement is on the licensee's process to identify changes made to such equipment that could potentially affect the implementation of the protective strategy. The licensee is expected to periodically review target sets for completeness and continued

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

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

The proposed rule attempted to address all access controls equally without addressing specific implementing differences for access to the owner controlled area, PA, or vital areas (VA). The Commission received several comments to clarify these differences in access controls for each area regarding processing of materials, personnel, and vehicles. The Commission agrees and the final rule is revised to address access control requirements for each area. The Commission also revised § 73.55(g)(1)(ii), (A), (B), and (C) to clarify generic control measures for controlling vehicle access through a vehicle barrier. Section 73.55(g)(2) is revised to specifically address PA access controls, and § 73.55(g)(4) is revised to specifically address VA access controls.

The proposed § 73.55(g)(1)(iv) to monitor and ensure the integrity of the licensee's access control systems is deleted from the final rule because it is sufficiently addressed by §§ 73.55(n)(1)(i) and (g)(1)(i)(C). The rule requires that the licensee will ensure that all access controls are working as intended and have not been compromised such that a person, vehicle, or material is able to gain unauthorized access beyond a barrier.

The proposed § 73.55(g)(5) is renumbered as § 73.55(g)(3). The Commission received a comment that the proposed § 73.55(g)(3)(ii) would have relaxed the requirement for armed security escorts for all vehicles inside a nuclear power plant's PA or VAs, unless the vehicle was specifically designated for use in such areas. The commenter further stated that the provision provides no explanation for the proposed change to this requirement, particularly given that there appears to have been no change in the threat environment that might warrant this change in security.

The Commission disagrees that requirements for control of vehicles inside the PA are relaxed by this requirement. The pre-existing requirement § 73.55(d)(4) did not require an armed escort for all vehicles but rather required only that the escort be a member of the security organization who may have been an unarmed watchman. The requirement has been revised,

however, to permit the use of non-security-organization personnel as escorts for vehicles except that armed security personnel must escort vehicles containing hazardous materials and unsearched bulk items. Vehicle escorts, however, must be trained in accordance with the licensee's training and qualification plan as required by § 73.55(g)(8)(iii).

The pre-existing requirement for licensees to designate certain vehicles for use inside the PA has been deleted from the final rule. The Commission concluded that simply designating a vehicle for use inside the PA is an unnecessary regulatory burden and, therefore, is not necessary. Section 73.55(g)(3)(iii) requires that vehicle use inside the PA must be limited to plant functions or emergencies and that keys must be removed or the vehicle otherwise disabled when not in use. All vehicles and personnel must be searched before entering the PA. Vehicles operated by individuals who are authorized unescorted access to the PA are not required to be escorted.

The proposed § 73.55(g)(4)(ii)(C), which would have required licensees to implement procedures during an emergency to ensure that the licensee's capability to prevent significant core damage and spent fuel sabotage was maintained, is deleted because it is sufficiently addressed by § 73.55(b)(3).

The proposed § 73.55(g)(4)(iii) is subsumed by §§ 73.55(g)(5)(ii) and 73.55(b)(11). These provisions require that consideration be given to how access to and egress from the site will be controlled during an emergency, which is a function assigned to the security organization consistent with site emergency procedures.

The Commission received comments that passwords are not access control devices and, therefore, are not appropriate for the requirements of the proposed § 73.55(g)(6). The Commission disagrees. The Commission has determined that in physical security, passwords are a form of access control device because they are used to control access to security computer or electronic systems and may be used to control access to secured areas. The rule

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

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

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

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

person(s) to be escorted are authorized to perform. For those instances where the licensee uses facility personnel other than a member of the security organization to perform escort duties within the physical protection program, such as a vehicle escort, these individuals must be trained, equipped, and qualified in accordance with the security Training and Qualification Plan to perform this specific duty. The rule requires that facility personnel who are not members of the security organization will be trained and qualified for the specific physical protection duties that they are assigned which includes possessing the knowledge, skills, abilities, and the minimum physical qualifications such as sight, hearing, and their general health needed to perform the assigned duties effectively.

The Commission received another comment that the proposed § 73.55(g)(8) allows escorts to take multiple visitors with no background checks into PAs and VAs, but does not require that the escorts meet even minimal physical and visual capabilities. The commenter stated that, unlike the proposed new requirement in Part 73, appendix B, paragraph B.2.a(2) that unarmed members of the security organization meet specified physical capabilities, the proposed regulations in § 73.55(g)(8) would not prevent licensees from assigning blind, deaf, and mute persons as escorts. The commenter urged that the regulation define minimally acceptable physical attributes for escorts. The Commission disagrees with this comment. The final rule does not require personnel escorts to be subjected to medical qualifications to perform escort duties but does require escorts to meet the requirements of § 73.55(g)(8), which establishes training and qualification requirements for personnel escorts. Further, personnel escorts are required to be capable of performing the assigned duty and maintain communication with the security organization when performing escort duties to summon assistance if needed. The NRC has never imposed minimum physical qualifications on licensee personnel escorts and the commenter has supplied no basis to impose such requirements now.

Section § 73.55(g)(8)(i) through (v) updates pre-existing requirements consistent with

Commission expectations and current licensee practices for performing escort duties. The Commission received several comments that the proposed § 73.55(g)(8)(ii), which would have required that individuals assigned escort duties be provided a means of "timely communication," was without basis because current communications capabilities at facilities are sufficient for escorts to make notifications or requests for assistance. Therefore, the commenter asserted that the NRC should delete this provision from the final rule. The Commission disagrees. The rule requires that escorts be able to call for assistance when needed. The "timely communication" language in the final rule does not require a specific form of communication media. It is the responsibility of each licensee to determine the appropriate communication media for their site which may or may not include the use of hand-held radios, public address systems, intercoms, etc. The Commission has concluded that timely communication capability is an appropriate update to pre-existing requirements and current licensee practices. Therefore, the Commission retains this requirement in § 73.55(g)(8)(ii).

The Commission received several comments that the proposed § 73.55(g)(8)(iii) for continuous communication is a new requirement without basis. The Commission disagrees. Section 73.55(g)(8)(iii) is an appropriate update to the pre-existing requirement described in § 73.55(f)(1), which required security personnel to maintain *continuous* communication capability with the central and secondary alarm stations and the pre-existing § 73.55(d)(4) which required vehicles to be escorted by security personnel while inside the PA. Section 73.55(g)(3)(ii) relieves the licensee from the pre-existing § 73.55(d)(4) and allowed non-security personnel, who are trained and qualified in accordance with the security Training and Qualification Plan, to escort vehicles inside the PA. In providing this relief, the Commission concluded that it is prudent to "retain" the pre-existing § 73.55(f)(1) requirement for vehicle escorts to maintain a continuous communication capability that was otherwise present through the use of security personnel escorting vehicles. It is also important to note that § 73.55(g)(8)(iii) is revised to

permit vehicle escorts to directly contact members of the security organization other than the CAS or SAS for assistance. The proposed requirement would have limited this communication to only the CAS or SAS.

The Commission received a comment that the proposed § 73.55(g)(8)(iv) phrase "knowledgeable of those activities that are authorized to be performed within the areas" is broad and impracticable and that escorts should only be responsible for observing obvious indications of inappropriate behavior. The Commission agrees in part and revised § 73.55(g)(8)(iv) to clarify that the level of knowledge required is general and that general knowledge of authorized activities is a fundamental requirement for an effective escort.

The Commission received comments that proposed § 73.55(g)(8)(v), which described minimum visitor to escort ratios in protected and vital areas, would not have provided sufficient protection against the possibility that visitors could attempt to commit or facilitate acts of radiological sabotage. The Commission disagrees that the requirements reflected in the proposed rule are not sufficient to ensure that visitor activities are adequately controlled, and they are, therefore, reflected in the final rule. The rule requires each licensee to implement visitor observation and control measures that are consistent with the physical protection program design requirements in § 73.55(b) including specific requirements for searches of personnel, escorting of personnel, and escort communications. The Commission has concluded that the visitor control measures required by this paragraph provide an appropriate level of protection and prescribing specific visitor-to-escort ratios is unnecessary. Visitor-to-escort ratios should be specific to each site and visitor based on site conditions and the rationale for the visit. Therefore, § 73.55(g)(8)(v) is revised to delete the proposed visitor-to-escort ratios (10 to 1 in the PA and 5 to 1 in VAs) as these ratios are addressed in regulatory guidance and required to be delineated in the licensee's NRC-approved security plans.

Section 73.55(h), Search Programs. The Commission received several comments that

search requirements should be addressed according to facility area (i.e., owner controlled area (OCA) and PA). The Commission agrees, and § 73.55(h) has been revised to address search requirements by area. This revision is necessary to clarify the differences of search requirements and implementation for owner controlled and protected areas.

The Commission received several comments to clarify the proposed § 73.55(h)(1) and (1)(i) regarding searches and that searches should be conducted at each physical barrier only for those items that must be excluded beyond the barrier. The Commission agrees that clarification is warranted and has combined and renumbered the proposed § 73.55(h)(1) and (h)(1)(i) as § 73.55(h)(1). Consistent with § 73.55(b)(4), each licensee must analyze their site-specific conditions to determine what personnel, vehicles, and materials must be prevented from gaining access to specific areas of the facility and will search the personnel, vehicles, and materials to satisfy the design requirements of § 73.55(b).

The proposed § 73.55(h)(5) is renumbered as § 73.55(h)(2)(iii). Section 73.55(h)(2)(iii) is revised to specify implementing details for the conduct of vehicle searches within the OCA including to the number of personnel required and the duties to be performed by each. The search process applied in the OCA must be performed by two personnel at least one of which must be armed and positioned to observe the search to provide an immediate response if needed. The rule requirement for searches conducted at vehicle checkpoints within the OCA is that one individual will conduct the search function, a second armed individual will be physically located at the checkpoint to provide an immediate armed response if needed, and a third individual, in accordance with § 73.55 (h)(2)(v), will monitor the search function via video equipment at a location from which that individual can initiate an additional response.

The proposed § 73.55(h)(8) through (h)(8)(iii) are renumbered as § 73.55(h)(3)(v) through (h)(3)(viii). The Commission received a comment that Commission approval of exceptions to search requirements through licensee security plans is unreasonable and

unnecessary. The Commission agrees in part, and § 73.55(h)(3)(v) is revised to clarify the rule requirement that a general description of the types of exceptions must be stated in the licensee security plans rather than a specific listing of individual exceptions which must be captured in procedures.

The proposed § 73.55(h)(8)(i) is renumbered as § 73.55(h)(3)(vii). The Commission received a comment that the requirement for an armed escort is not applicable in all cases. The Commission agrees in part and has revised § 73.55(h)(3)(vii). The rule requires that bulk items excepted from the search required for access into the PA will be escorted by an armed member of the security organization to ensure that unsearched bulk items are controlled until they can be offloaded and the absence of contraband can be verified to the extent practicable.

The proposed § 73.55(h)(1)(iii) is subsumed in the final rule in appendix B of part 73.

The proposed §§ 73.55(h)(2)(i) and 73.55(h)(2)(ii) regarding clearly identifying items during a search are subsumed as §§ 73.55(h)(2)(iv) and 73.55(h)(3)(i).

Section 73.55(i), Detection and Assessment Systems. Several requirements from proposed §§ 73.55(i)(7) and 73.55(i)(10) have been consolidated, revised, relocated, and/or deleted to eliminate redundancy and provide clarification for alarm annunciation and video assessment equipment in both alarm stations and have been designated as § 73.55(i)(2) and (3).

The proposed §§ 73.55(i)(4), 73.55(i)(4)(i), and 73.55(b)(3) are combined and renumbered as § 73.55(i)(4)(i). The Commission received a comment that the requirements set forth in the proposed § 73.55(i)(4) were significant high-impact requirements that exceed the existing requirements without basis and whose exact scope and impact could not be assessed with the current language. The Commission agrees that further clarification of the intent and scope of these requirements is necessary. In the final rule, the pre-existing requirement in § 73.55(e)(1) for protection of at least one alarm station against a single act is retained.

Section 73.55(i)(4)(i) of the final rule clarifies the functions that must survive from a single act by requiring licensees to ensure the survivability of either alarm station to maintain the ability to perform the following four functions: detection and assessment of alarms, initiation and coordination of an adequate response to alarms, summoning offsite assistance, and providing effective command and control. The proposed § 73.55(b)(3), which generally addressed the protection of personnel, systems, and equipment from a single act bounded by the design basis threat, is now reflected as § 73.55(e)(10)(i)(A), which generally describes licensee measures for protection against the design basis threat land vehicle bomb assault. A single act does not refer to the number of acts committed during a security contingency event; rather it pertains to any one act that alone could remove the licensee's capability to retain at least one alarm station and/or its functions as required. An example of a single act against which this regulation requires protection would be destruction of security equipment not specifically accounted for in the licensee protective strategy that is accessible from the PA perimeter and that its destruction would remove the capability to retain one alarm station and/or its required functions.

The proposed § 73.55(i)(4)(ii) is renumbered as § 73.55(i)(3)(vii). The Commission received several comments that proposed § 73.55(i)(4)(ii), which would have required uninterruptable backup power for all alarm station functions, would be a significant high-impact requirement that would exceed the existing requirements without a basis and that the exact scope and impact of the requirement cannot be assessed with the current language. The Commission agrees in part, and has revised § 73.55(i)(3)(vii) to clarify the scope of equipment to which this requirement applies. The Commission recognizes that because the transfer to secondary power is not an instantaneous event, the maintenance of continuous power to some equipment essential to the initiation of licensees' protective strategies may not be possible and could result in a period of degraded performance. In light of this potential vulnerability, the rule requires uninterrupted power supplies for detection and assessment equipment at the PA

perimeter to ensure continued operability in the event of the loss of normal power during the transition between normal power and initiation of secondary power. The Commission determined that a licensee's capability to detect and assess a threat at the PA perimeter is an essential function for all sites, and as such, the equipment needed to satisfy the requirement in § 73.55(i)(1) must remain operable through an uninterruptible power supply. Based on each licensee's site specific considerations, detection and assessment equipment subject to this requirement may, for example, include alarm annunciators and sensors, lighting, closed circuit televisions, and video image recording necessary to provide detection and assessment at the protected area perimeter. However, under this rule, each license must identify which detection and assessment equipment it relies on to initiate its protective strategy. This requirement is based on the pre-existing § 73.55(e)(1), the evaluation of information gained through enhanced baseline inspections and force-on-force exercises.

Section 73.55(i)(4)(ii)(E) is added to ensure that licensees address events (e.g., trespassing) that may not require a response in accordance with the protective strategy but may require the employment of elements within the licensee's force continuum and legal authority as permitted under applicable State law.

Section § 73.55(i)(4)(ii)(G) is added for consistency with § 73.55(i)(4)(ii)(F) to ensure that operators in both alarm stations are knowledgeable of the final disposition of all alarms, thus minimizing the possibility of assessment errors.

The proposed §§ 73.55(a)(6), 73.55(a)(6)(i), and 73.55(a)(6)(ii) are consolidated and re-numbered as § 73.55(i)(4)(iii). The Commission received several comments to clarify the applicability and scope of the proposed § 73.55(a)(6) and to relocate this requirement to § 73.55(i). The Commission agrees that additional clarity is needed but declines to relocate the applicability language in § 73.55(a)(6). Sections 73.55(a)(6) and 73.55(i)(4)(iii) specify that the requirement to construct, locate, protect, and equip both the central and secondary alarm

stations (CAS and SAS) is applicable to only applicants for an operating license under the provision of part 50 or holders of a combined license under the provisions of part 52 that is issued after the effective date of this rule. The rule requires that both alarm stations for new reactors will be equal and redundant and will meet construction standards previously applied only to the CAS. Specifically, the Commission has deleted the pre-existing provision that otherwise permitted the SAS to be located offsite. Operating power reactors licensed before the effective date of this final rule and the Tennessee Valley Authority's Watts Bar Nuclear Plant need not renovate their existing alarm stations to meet this requirement. Applicants for a new operating license or combined license for a reactor that would be constructed inside an existing PA must construct both the CAS and SAS to the requirements of § 73.55 for CAS, unless otherwise exempted through established licensing processes.

The proposed §§ 73.55(i)(5), (i)(6), and (i)(7)(i) related to detection and assessment capabilities are deleted because they are subsumed as § 73.55(i)(1) which provides a general description of detection and assessment requirements.

The proposed §§ 73.55(i)(9)(ii), (ii)(A), and (ii)(B) are combined and renumbered as § 73.55(i)(5)(ii). The Commission received a comment that the NRC should delineate the requirements of each of the three areas (OCA, PA, and VA) in the final rule and clarify what is meant by the proposed "integrity of physical barriers or other components." The Commission agrees and the final rule is revised to clarify that this requirement applies to the OCA. The term "integrity" is retained and is meant to refer to the ability of the barrier to perform its function and that it has not been tampered with.

The proposed § 73.55(i)(9)(iv) is renumbered as § 73.55(i)(5)(iii). The Commission received several comments to clarify the proposed § 73.55(i)(9)(iv), which concerned licensee obligations for observation of unattended unmonitored openings. The Commission agrees that clarification is needed, and § 73.55(i)(5)(iii) is revised to clarify that this requirement focuses on

monitoring unattended openings, such as underground pathways, that can be exploited to circumvent the intent of a barrier or otherwise defeat its required function.

The proposed § 73.55(i)(9)(iii)(B) has been divided and renumbered as § 73.55(i)(5)(v) and (vi). The Commission received a request for clarification of the intent of the proposed requirement specific to “random intervals.” The Commission agrees and § 73.55(i)(5)(vi) is revised to clarify the scope of patrols relative to PAs, VAs, and target sets. The term “random” as used in the final rule is not intended to describe the periodicity of the patrols but to describe the manner in which the patrol is conducted to prevent predictability.

The proposed § 73.55(i)(9)(iii)(C) is renumbered as § 73.55(i)(5)(vii). The Commission received several comments to add the word "obvious" before the word tampering because security personnel generally do not possess the level of specific knowledge that might be necessary to detect the types of tampering that could have been included within the scope of the rule. These commenters noted that other licensee operations personnel who possess detailed engineering knowledge also provide observation of target set equipment and additional assurances that tampering would be identified. The Commission agrees and § 73.55(i)(5)(vii) is revised to include the term “obvious” consistent with the level of knowledge that security personnel possess regarding plant operations based on training that is provided to them.

The proposed §§ 73.55(i)(10) and (i)(10)(i) are deleted from the final rule because this proposed requirement to maintain video equipment in operable condition is redundant to §§ 73.55(b)(3) and 73.55(n)(1)(i).

The proposed § 73.55(i)(10)(iii) is deleted from the final rule. The NRC received a comment that ensuring personnel assigned to monitor video equipment are alert and able to perform their assigned duties is a licensee management responsibility. The Commission agrees. Fitness-for-duty, fatigue, and work-hour controls are covered in 10 CFR part 26.

The proposed § 73.55(i)(11)(i) is renumbered as § 73.55(i)(6). The Commission

received several comments to clarify this lighting requirement. The Commission agrees and § 73.55(i)(6) is revised to clarify the lighting requirements and identify acceptable alternatives. The reference to the OCA is removed from this paragraph as it is duplicative to the reference in § 73.55(b).

The proposed § 73.55(i)(11)(ii) is renumbered as § 73.55(i)(6)(ii). The Commission received several comments to clarify the pre-existing requirement for 0.2-foot-candle illumination and the application of low-light technology. Consistent with the proposed rule, the current 0.2-foot-candle illumination requirement is explicitly retained as the minimum standard for illumination levels at nuclear power reactor facilities. However, § 73.55(i)(6)(ii) is revised to clarify and introduce the use of low-light technology to supplement the facility lighting scheme and to provide the flexibility needed for licensees to use low-light technology. The rule requires that licensees will ensure that lighting levels either meet the 0.2-foot-candle requirement, or employ low-light technology to ensure the protective strategy can be implemented effectively.

Section 73.55(j), Communication Requirements. The Commission has made no significant changes to § 73.55(j). The Commission received a comment that proposed § 73.55(j)(1), which would require the maintenance of continuous communication with offsite resources, was without a basis. The commenter argued that the ability to maintain such communication is beyond the ability of licensees. The Commission disagrees. This requirement is retained from the pre-existing § 73.55(f)(3) and remains unchanged. The rule requires that each licensee security organization maintains continuous communication with local law enforcement authorities and onsite personnel.

The Commission received a comment that proposed § 73.55(j)(4)(iii), regarding the licensee's communication system, is not appropriate for escorts. The Commission agrees and § 73.55(j) is revised to address the specific communication requirements of personnel or entities requiring communications and communication systems to be employed to meet the requirement.

The rule requires that vehicle escorts are provided by the licensee with the appropriate means to call for assistance when needed. The final rule does not require a specific form of communication media, and therefore, it is the responsibility of each licensee to determine the appropriate communication media for their site which may or may not include the use of hand-held radios, public address systems, intercoms, etc.

The Commission received a comment that proposed § 73.55(j)(6), which would have required the licensee to identify and establish alternative communication methods for areas of its facility where communication could be interrupted or not maintained, was without a basis, and would be virtually impossible to implement given a power plant's reinforced concrete construction and trip sensitive equipment. The Commission disagrees and believes that the commenter misinterpreted the Commission's intent. A condition as described in the rule, if present at a site, must be identified and accounted for to satisfy the pre-existing § 73.55(f)(1) requirement for continuous communication. However, the Commission does not intend to require that such conditions be "fixed" but rather that the licensee compensate for this condition as needed and appropriate for their site-specific considerations.

Section 73.55(k), Resource Requirements. The proposed §§ 73.55(k)(1)(ii) and (iii), regarding the training and qualification of armed responders and the availability of certain equipment, are deleted from the final rule. These requirements are sufficiently addressed in the final rule in appendix B to part 73 and appendix C to part 73 and, therefore, are redundant.

The proposed § 73.55(k)(1)(iv), regarding training for assigned weapons, is renumbered as § 73.55(k)(2). The Commission determined that the proposed § 73.55(k)(3)(iv) is redundant to this requirement and has revised § 73.55(k)(2) to clarify performance criteria.

The proposed requirement in § 73.55(k)(1)(v) regarding weapons training and qualification of armed responders is deleted from the final rule because it is redundant to the requirements set forth in appendix B to part 73.

The proposed § 73.55(k)(3) is renumbered as § 73.55(k)(4). The final rule § 73.55(k)(4) is clarified to delineate the duties of armed responders and armed security officers. Section 73.55(k)(5) is added to retain the pre-existing requirement, described in former § 73.55(h)(3), for the minimum number of armed responders required to be immediately available at the facility to fulfill response requirements. The rule requires that each licensee will determine the specific minimum number of armed responders needed to protect their facility and that under no circumstances will that minimum number be less than 10 inside the PA and available at all times.

The proposed § 73.55(k)(3)(iii) and (iv) are deleted from the final rule. The Commission concluded that these proposed requirements are redundant to the final rule appendix B to part 73 and § 73.55(n)(1)(i), respectively.

The proposed § 73.55(k)(6) regarding licensee personnel being trained to understand their roles during security incidents, is deleted from the final rule. The Commission has determined that this requirement is more appropriate for site procedures and has deleted it from the final rule.

The proposed § 73.55(k)(7)(iv) is renumbered as § 73.55(k)(8)(iii). The Commission received a comment that it does not have a basis to require licensee notification of offsite agencies other than local law enforcement upon receipt of an alarm or other threat notification. The Commission generally agrees that the requirement is not necessary. Section 73.55(k)(8)(iii) is revised to specify that licensees must notify local law enforcement only in accordance with their site procedures. However, as noted below, some licensees have established liaison with non-local law enforcement agencies including State or Federal. To the extent that these arrangements are noted in those licensees' site procedures, the rule would require their notification.

The proposed § 73.55(k)(8) is renumbered as § 73.55(k)(9). The Commission received a

comment that it does not have a basis to require licensees to obtain liaison agreements with agencies other than local law enforcement. The Commission disagrees with this comment but has clarified the rule. In some instances, licensees have arrangements with agencies not considered "local law enforcement" such as Federal or State law enforcement agencies. It is, therefore, an appropriate update to the regulatory framework to include the possibility of State and Federal law enforcement agencies as well as local law enforcement to account for sites whose local law enforcement are State or Federal agencies. However, such agreements are not required by the rule. Further, the Commission acknowledges that in some cases a local, State, or Federal law enforcement agency cannot or will not enter into a written agreement with a licensee, and in such cases the Commission's expectation is that the licensee will make a reasonable effort to pursue liaison with these agencies to the extent practicable and that this liaison is documented.

The proposed appendix C to part 73, section II, paragraph (k), "Threat Warning System," paragraph (k)(1), (k)(2), and (k)(3) are moved and renumbered as §73.55(k)(10), paragraph (k)(10)(i), and paragraph (k)(10)(ii). The Commission concluded that these requirements are better presented in the regulatory framework for the physical protection program. The rule requires that the licensee will pre-plan specific enhancements to their physical protection program to be taken upon notification by the NRC of a heightened threat environment.

Section 73.55(l), Facilities Using Mixed-Oxide (MOX) Fuel Assemblies Containing up to 20 Weight Percent Plutonium Dioxide ($PuO_2$). The Commission received a comment that through this proposed rulemaking, the NRC is ignoring the Atomic Safety and Licensing Board's (ASLB) decision in the Catawba case. The commenter stated that, in that case, the ASLB added security conditions to Duke Energy's proposed security plan at Catawba and that one of the ASLB's conditions is not in the proposed rule. The Commission disagrees with this

assertion. In fact, the Commission specifically rejected the ASLB's imposition of additional license conditions for the use of MOX fuel and affirmed the staff's conclusion that the additional security measures provided by the licensee would provide reasonable assurance of the protection of public health and safety in light of the theft risk presented by the use of MOX fuel (*Duke Energy Corp.* (Catawba Nuclear Stations, Units 1 and 2), CLI-05-14, 61 NRC 359 (2005)). The Catawba license amendments were issued on March 3, 2005 (70 FR 11711; March 9, 2005). The requirements described in § 73.55(l) are consistent with the physical protection program enhancements that were applied to the Catawba facility. Section 73.55(l) is revised to clarify that those licensees choosing to use MOX fuel assemblies must implement additional measures designed to prevent theft or diversion of un-irradiated MOX fuel assemblies in addition to protecting the power reactor facility against the design basis threat of radiological sabotage.

The Commission received a comment that the NRC did not define MOX fuel in the proposed rule (with regard to concentration, weight, or any other physical property), and suggested that this is necessary. The Commission agrees, and § 73.55(l) is revised to specify the maximum percent weight of plutonium dioxide allowed within a MOX fuel assembly and that the use of MOX fuel assemblies with percent weights greater than 20 weight percent plutonium dioxide require unique and separate approval from the Commission. In such cases, licensees would be required to submit a license amendment request, and the Commission would consider additional security measures as necessary. Section 73.55(l)(3)(v)(B) is also revised to clarify the number of physical barriers required for protection of un-irradiated MOX fuel assemblies. Physical protection of un-irradiated MOX fuel assemblies requires three physical barriers of which the water contained within the spent fuel pool is the third barrier.

Finally, the commenter disagreed with the fact that the proposed rule language did not make a distinction between the security applied to a small number of MOX lead test assemblies and the security applied to a large number of assemblies. The Commission disagrees that such

a distinction is necessary in the rule. Because the Commission considers only one part of one assembly to be the goal quantity of a theft scenario and because theft of only a portion of the fuel in one assembly would be considered failure, no additional protection would be added by distinguishing between multiple additional assemblies. The physical protection program requirements specified in § 73.55(l) are appropriate for any quantity of unirradiated MOX fuel assemblies that are less than or equal to 20 weight percent plutonium dioxide and may be on-site at any time.

Section 73.55(m), Security Program Reviews. The proposed § 73.55(m) for "Digital computer and communication systems and networks" is relocated to a stand-alone section (10 CFR 73.54). The Commission has determined that these requirements are best addressed as a stand-alone section similar to the requirements for an access authorization program.

The proposed § 73.55(n) is renumbered as § 73.55(m) to account for the renumbering of the proposed § 73.55(m) as 10 CFR 73.54.

The proposed §§ 73.55(n)(1) and (n)(1)(ii) are combined and renumbered as § 73.55(m)(1). The Commission received a comment to clarify the periodicity of audits and reviews required by proposed § 73.55(n)(1). Section 73.55(m)(1) is revised to clarify periodicity. The rule requires that each licensee will review their physical protection program to determine if the programmatic requirements established are being implemented. The rule also requires that each licensee will review the physical protection program to determine if the physical protection program effectively meets Commission requirements. The licensee must ensure that all components or elements of the physical protection program are reviewed at intervals no less than every 24 months. However, the Commission has concluded that licensees must also review individual components or elements of the physical protection program no later than 12 months following a significant change to site-specific conditions, equipment, personnel, or other performance indicators.

The proposed §§ 73.55(n)(3) and (4) are deleted because these requirements are redundant to the requirement to review the physical protection program at intervals not to exceed 24 months.

The proposed § 73.55(n)(5) is deleted because it is redundant to the final rule Part 73, appendix B, Section VI, for the performance evaluation program.

The proposed § 73.55(n)(8) is deleted because the requirements for the site corrective action program as stated in § 73.55 (b)(10) address all issues, not just findings from reviews, audits, etc. as stated in the proposed rule.

The proposed § 73.55(n)(9) is deleted because this provision does not apply to reviews and audits addressed herein and is limited to only the conduct of training program requirements addressed in part 73, appendix B, Section VI.

Section 73.55(n), Maintenance, Testing, and Calibration. The proposed § 73.55(o) is renumbered as § 73.55(n) to account for the renumbering of the proposed § 73.55(m) to a stand-alone section (10 CFR 73.54).

The proposed § 73.55(o)(1)(i) is renumbered as § 73.55(n)(1)(i). The Commission received a comment asking who determines the “predetermined intervals” in which testing and maintenance are required. The predetermined intervals for maintenance, calibration, and performance testing of equipment are specified by manufacturer specifications and the NRC. The Commission has concluded that specific, pre-determined intervals for operability testing are required to ensure that certain equipment is capable of performing its intended function.

Section 73.55(o), Compensatory Measures. The proposed § 73.55(p) is renumbered as § 73.55(o) to account for the renumbering of proposed § 73.55(m) for cyber security requirements to a stand-alone § 73.54.

Section 73.55(p), Suspension of Security Measures. The proposed § 73.55(q) is renumbered as § 73.55(p) to account for the renumbering of proposed § 73.55(m) for cyber

security requirements to a stand-alone § 73.54.

The Commission received a comment that proposed § 73.55(q)(1)(ii) requires that a licensed senior operator approve the suspension of safeguards measures. The commenter suggested that approval from a licensed senior operator was excessive and that the rule should be revised to permit approval by the "on shift operations manager." The Commission disagrees and finds that approval by a licensed senior operator is appropriate for all suspensions of security measures pursuant to § 73.55(p). The allowance for suspensions of security measures for severe weather conditions is based on the pre-existing §§ 50.54(x) and (y) which explicitly requires, at a minimum, approval by a licensed senior operator. Under this provision, the security supervisor recommends when security measures must be suspended; and, consistent with the pre-existing §§ 50.54(x) and (y), a licensed senior operator must, at minimum, approve that decision to ensure that other operational and safety concerns have been fully considered and that there will be no adverse affects or undue risk to the public health and safety as a result of the suspension.

The proposed § 73.55(q)(4) is deleted because the requirement to report the suspension of safeguards measures is redundant to § 73.71 and is sufficiently addressed in § 73.55(p)(3).

Section 73.55(q), Records. The proposed § 73.55(r) is renumbered as § 73.55(q) to account for the renumber of proposed § 73.55(m) for cyber security requirements to a stand-alone section (10 CFR 73.54). The proposed § 73.55(d)(5) is renumbered as § 73.55(q)(3) to retain the requirement for retention of security force contracts as a record for the duration of the contract and retention of superseded portions for three years following changes to that contract.

Section 73.55(r), Alternative Measures. The proposed § 73.55(s) is deleted because it is redundant to § 73.58. The Commission has determined that safety/security interface is a stand-alone section, the applicability of which is adequately addressed in § 73.58 and need not be referenced in § 73.55 to ensure clarity or applicability.

The proposed § 73.55(t) is renumbered as § 73.55(r) to account for the renumbering of the proposed § 73.55(m) for cyber security requirements to a stand-alone section (10 CFR 73.54) and the deletion of proposed § 73.55(s) "Safety/security interface." Section 73.55(r) represents the same set of requirements that were described in former § 73.55(a), which stated, in part, "the Commission may authorize an applicant or licensee to provide measures for protection against radiological sabotage other than those required by this section…." That provision had been known as the "alternative measures" provision although that specific phrase did not appear in the rule text. The final rule codifies that phrase as it relates to this process, but the requirements of seeking and obtaining approval for an "alternative measure" essentially remains as it had been set forth in the existing rule.

**F. Section 73.56, Personnel Access Authorization Requirements for Nuclear Power Plants.**

General Comments. Section 10 CFR 73.56, the Commission has revised the proposed rule text and associated statement of considerations to (1) address over 180 pages of the comments received on the proposed rule, (2) provide additional clarifications and specifications, and (3) correct errors. The following provides a brief explanation of the significant changes to the proposed rule and the Commission's responses to the comments.

The Commission received numerous comments on the proposed rule as a result of unclear descriptions or inconsistent use of the roles and responsibilities of licensees, applicants, and contractors or vendors and the phrases "grant unescorted access" and "authorize unescorted access authorization."

In response to the comments received and suggestions implicit in the comments received on various provisions in the proposed rule, the Commission improved the clarity and precision of the final rule by providing the following clarification in the statement of consideration for § 73.56(a). First, the Commission replaced the phrases "unescorted access authorization"

and “access authorization” with the phrases “unescorted access” and/or “unescorted access authorization” to correct misuse and misinterpretation of the rule. Second, the Commission replaced the term “grant” associated with “unescorted access authorization” and “access authorization” with the terms “grant” and/or “certify.” Finally, the Commission made several revisions in order to provide clarification and/or specifications on the roles and responsibilities of licensees, applicants, and contractors or vendors.

Additionally, the Commission revised paragraphs (a)(4) and deleted (a)(5) in the final rule to define and to provide clarification and specification on the roles and responsibilities of licensees, applicants, and contractors or vendors. Throughout the final rule, the Commission revised the proposed rule text to reflect the above clarifications and specifications.

Throughout the proposed rule text, the Commission received comments that some of its statements in the proposed rule regarding the accessibilities and capabilities of the information-sharing mechanism that the industry is currently using to comply with the Commission’s requirements were incorrect. Specifically, commenters noted that the information-sharing mechanism used by the industry does not contain records, but rather it contains data representative of the records that are accessed and controlled by licensees, applicants, and certain contractors or vendors. The Commission agrees with the received comments and revised the final rule to clarify that use of an information-sharing mechanism is not a requirement; rather it is the sharing of specific access authorization information with the other licensees subject to this section that is required in accordance with § 73.56(o)(6).

Section 73.56(a), Introduction. The Commission deleted proposed paragraphs (a)(2) and (a)(3) pertaining to the submission of access authorization program amendments for Commission approval and the continued implementation of the access authorization program under current requirements in the final rule as those requirements have been incorporated in § 73.56(a)(1).

Section 73.56(b), Individuals Subject to the Access Authorization Program. Commenters stated that proposed paragraph (b)(1)(ii) does not contain a necessary provision that allows for short-term escorted digital access and addresses access authorization requirements for an individual accessing emergency response components that include commercial facilities that are not subject to access authorization requirements. The Commission disagrees with the recommended rule requirements. The Commission finds that these comments are beyond the scope of this rule because this section specifically provides for requirements for unescorted access and unescorted access authorization for protected and vital areas of nuclear power plants and to these entities only. This section does not cover escorted digital access; however, cyber security requirements are covered in § 73.54. Therefore, the NRC did not make any revision to the rule text.

Section 73.56(c), General Performance Objective. The Commission received comments that the requirements set forth in proposed § 73.56 (d)(3) regarding identity verification requirements, did not properly consider the North America Free Trade Agreement, which allows Canadian citizens performing certain services to enter the United States without either an alien registration or an I-94 Form. The commenters also stated that the proposed rule text incorrectly allowed contractors or vendors to evaluate the results of fingerprinting required under § 73.57. The Commission agrees with the received comments and revised the proposed rule text to allow licensees and applicants to use an alien registration or an I-94 Form to verify the identity of a foreign national. Additionally, the NRC deleted the requirement that required contractors or vendors to evaluate the results of fingerprinting required under § 73.57, and now only licensees or applicants may do so.

The Commission received comments that the phrase, “full credit history evaluation” stated in proposed § 73.56(d)(5) needs additional clarification and specification by providing a time period for credit history. The comments also stated that fraud check should be deleted

from credit history checks and that credit history checks, or other financial documentation, should be required for foreign nationals in the final rule. The Commission agrees in part and disagrees in part with the comments. The Commission disagrees with specifying the time period for a credit history evaluation and deleting fraud checks from the credit history check as the Commission notes that the requirements set forth in this paragraph are consistent with the requirements set forth in the 2003 order and with current industry practice. Further, the full credit history evaluation requirements reflect the Commission's intent that all financial information available through credit-reporting agencies is to be obtained and evaluated because it has the potential to provide highly pertinent information. However, the Commission agrees with the commenter that the requirement should address credit history checks of foreign nationals. The Commission recognizes that certain foreign nationals' host countries may not have routinely accepted credit reporting mechanisms, and therefore, the Commission revised the final rule text to allow multiple sources of credit history that could potentially provide information about a foreign national's financial record and responsibility, not limited to routinely accepted credit reporting mechanisms.

The Commission revised proposed § 73.56(d)(7) to distinguish the criminal history records check requirements for those individuals who are expected to have unescorted access or unescorted access authorization. Individuals who are expected to have unescorted access must have a criminal history records check in accordance with the requirements of 10 CFR 73.57. However, the NRC cannot obtain a criminal history records check in accordance with § 73.57 for individuals not expected to have unescorted access because Section 149 of the AEA limits the NRC's ability to obtain fingerprints from those individuals. Instead, a criminal history records check of those individuals not expected to have unescorted access will be obtained in accordance with § 73.56(k)(1)(ii).

Section 73.56(e), Psychological Assessment. The Commission received comments that the term "clinical" should be removed from the phrase "a licensed clinical psychologist or psychiatrist" in proposed § 73.56(e)(1) pertaining to qualifications for psychologist or psychiatrists who conduct psychological assessments for trustworthiness and reliability. The commenter stated that psychologists or psychiatrists are licensed by states. However, some states might not issue licenses using the term "clinical" psychologists or psychiatrists. The Commission agrees with the comment and deleted the term "clinical" because the focus is on a psychologist or psychiatrist who has adequate experience, and that focus should not be limited by a particular term that some states may not use in their licensing procedures.

The Commission received comments that because proposed § 73.56(e)(2) would have required psychologists and psychiatrists to follow the ethical principles established by the American Psychological Association or American Psychiatric Association, the proposed regulation would limit the pool of available licensed and qualified psychologists and psychiatrists who can perform the required psychological assessments because these ethical principles might deviate from the ethical principles established by the states that license them and conflict with the requirements in proposed § 73.56(e)(3), which requires licensed psychologists and psychiatrists to have a face-to-face interview with an individual only after the individual surpasses predetermined thresholds on a psychological test. The commenter stated that § 73.56(e)(3) is, therefore, in conflict with the (e)(2) requirement to follow accepted ethical principles since part of the American Psychological Association's Ethical Principles and Code of Conduct mandates that psychologists interview in light of the research on or evidence of the usefulness of interviewing and would deviate from the ethical principles established by the American Psychological Association or American Psychiatric Association if it requires a psychological assessment that is not supported by research and for which the assessors are not properly trained.

The Commission disagrees with these comments. For the first comment, the Commission noted that the ethical principles established by the American Psychological Association or American Psychiatric Association specifically address the issues raised. These ethical standards require psychologists and psychiatrists to comply with the requirements of laws, regulations (including the requirements in section 73.56), or other governing legal authorities. Thus, the requirements set forth in this section do not deviate from the States' licensing requirements.

In response to the second comment, the Commission disagrees that §§ 73.56(e)(2) and (e)(4) are contradictory because Section 1.02 of "Ethical Principle of Psychologists and Code of Conduct" addresses this issue and states that, if a psychologists' ethical responsibilities conflict with law, regulations, or other governing legal authority, psychologists would have to take steps to resolve the conflict but must in any event adhere to the requirements of the law, regulations, or other governing legal authority.

In response to the third comment regarding sufficient demonstrated ability of psychological tests to help in the trustworthiness and reliability determination, the Commission directed the commenter to the considerable bodies of research in this area and pointed out a long track record of intelligence and other agencies that have used the Minnesota Multiphasic Personality Inventory – 2 (MMPI-2) as well as other personality tests for this purpose. Additionally, the Commission noted that a psychological assessment is only one of many access authorization program elements that licensees and applicants use for determining an individual's trustworthiness and reliability.

However, agreeing in part with the last comment, the Commission revised proposed § 73.56(e)(1) in the final rule to require psychologists or psychiatrists to be appropriately trained. Finally, the Commission is confident that the results of psychological testing, combined with the

results of other access authorization program elements, will yield high assurance regarding an individual's trustworthiness and reliability.

The commenters stated that proposed § 73.56(e)(3) should be revised to allow psychiatrists or psychologists to establish predetermined thresholds appropriate to the test and the target population that would be applied in interpreting the results to identify whether an individual shall be interviewed under § 73.56(e)(4)(i) of this section and interview the individual without administering the psychological test.

However, another commenter stated that establishing predetermined thresholds for the psychological test is not sufficient for establishing consistency among these psychological assessments. That commenter stated that psychologists or psychiatrists who perform psychological assessments must be properly trained. The Commission agrees with the first comment and revised the final rule to state that psychiatrists or psychologists shall establish the predetermined thresholds for each scale to determine whether an individual shall be interviewed. The Commission notes that it is appropriate and consistent with current professional practice for psychiatrists or psychologists, rather than the industry, to establish these threshold levels. However, the Commission disagrees with the second comment because the established thresholds for each scale must be applied equally and fairly to all individuals subject to the psychological assessment requirement, so a psychiatrist or psychologist may not waive this requirement in favor of an interview. Finally, the Commission agrees in part with the last comment and revised § 73.56(e)(1) to require that psychologists and psychiatrists be properly trained to ensure consistency among assessments.

The Commission received comments that proposed § 73.56(e)(5) would be too limiting and prescriptive in that it would make the reviewing official the focal point of a medical evaluation when licensees or applicants discover pertinent medical-related information about an individual who is being evaluated during an initial psychological assessment. One commenter

recommended that the Commission revise the proposed paragraph to avoid premature involvement of reviewing officials and therefore allow knowledgeable professionals to complete their evaluations and develop recommendations regarding the individual before involving the reviewing official. The Commission agrees with the commenters and revised the final rule to allow evaluation of the discovered medical information before reporting to the reviewing official.

While developing a response to the comments received in item 11 above, the Commission added § 73.56(e)(6) to address situations during a psychological reassessment where a psychologist or psychiatrist discovers any information, including a medical condition, that could adversely impact the fitness for duty, trustworthiness, or reliability of those individuals who are granted unescorted access or certified unescorted access authorization. The psychologist or psychiatrist must promptly inform the reviewing official, or the appropriate medical personnel, of this discovery to ensure that information is evaluated to determine that each person is trustworthy and reliable.

Section 73.56(f), Behavioral Observation. The Commission received comments that proposed §§ 73.56(f)(3) and (g) should be revised to allow individuals to report any concerns arising from a behavioral observation program or reportable legal actions to the reviewing official, the individual's supervisor or other management personnel designated in their site procedures. The Commission agrees. The Commission finds that individuals should be given options, with minimal restrictions, regarding to whom they can report any concerns that arise from a behavioral observation program or reportable legal actions by allowing an individual to report to the reviewing official, the individual's supervisor or other management personnel. However, if the recipient of the report is someone other than the reviewing official, that person must promptly convey the report to the reviewing official, who shall determine whether to maintain, administratively withdraw, or unfavorably terminate the reported individual's unescorted access or unescorted access authorization status.

Section 73.56(h), Granting Unescorted Access and Certifying Unescorted Access Authorization. To increase clarity in the organizational structure of the requirements set forth in § 73.56(h), the Commission reorganized §§ 73.56(h)(1), (h)(2), (h)(8), (h)(9), and (h)(10) to (h)(5), (h)(6), (h)(1), (h)(2), and (h)(3), respectively, in the final rule. Additionally, the Commission incorporated proposed §§ 73.56(h)(3), (h)(4), (h)(5), (h)(6), and (h)(7) into § 73.56(h)(4). The NRC has added the last two sentences in § 73.56(h)(4)(ii) to correct errors in proposed § 73.56(h)(3), which incorrectly listed reinstatement requirements for those individuals who last held unescorted access or unescorted access authorization that was terminated under favorable conditions within the past 30 days.

The Commission received two comments that proposed § 73.56(h)(8), stipulating the determination basis, needs to be revised to allow licensees to deny unescorted access to an individual as soon as the reviewing official receives information that would warrant such a decision even if the reviewing official has at that point not acquired all the information required by proposed § 73.56. The Commission agrees with the comment and revised § 73.56(h)(1)(ii) to reduce unnecessary regulatory burden by providing licensees and applicants the flexibility to terminate the process upon receipt of disqualifying information.

The Commission received two comments that proposed § 73.56(h)(10) should be revised to require the initial access authorization process for assessing individuals who have been in an access-denied status and prevent licensees who possess derogatory information about individuals from allowing those individuals any access, whether unescorted or escorted, to their protected areas.

The Commission agrees with the first comment and revised the final rule to delete reference to a re-instatement procedure by the licensee and to require that the initial access authorization process be used for adjudicating the access denied status consistent with current licensee practices. The Commission disagrees with the second comment. The Commission's

unescorted access requirements do not contain specific prescriptive disqualifiers for access; nor does the Commission believe it is prudent to add any. Licensees are required by § 73.56(h) to consider all of the information obtained in the background investigation as a whole in determining whether an individual is trustworthy and reliable before granting unescorted access. There is no particular piece of information that would automatically disqualify an individual from access. Furthermore, the commenter's suggestion that when licensees "possess" or "come across" such derogatory information the individual should be prevented from having any access is unworkable from a regulatory perspective. In order to avoid potential enforcement action, a licensee would be put in a position to conduct a full background investigation on an individual, which would undermine the entire purpose behind having the ability to escort visitors on site. The Commission does not see a basis to impose such a measure. The Commission has concluded that the requirements set forth in this section sufficiently address denial of unescorted access or unescorted access authorization based upon receipt of disqualifying information. The requirements for granting escorted access to visitors are sufficiently addressed in 10 CFR 73.55.

Section 73.56(i), Maintaining Unescorted Access or Unescorted Access Authorization. The Commission received three comments that proposed § 73.56(i)(1)(iv) should be revised. Commenters indicated that the Commission made improper reference to licensees' and applicants' Physical Security Plan for details about the Behavior Observation Program, should replace the term "interview" with the term "review" when referring to the "annual supervisory review" under which all individuals must undergo, and should use an "annual" supervisory review period rather than the phrase "nominal 12 months."

The Commission agrees with the first comment and revised the final rule to replace reference to the Physical Security Plan with reference to a licensee's Behavior Observation Program because details about the Behavior Observation Program, such as the annual supervisory review, are not found in the Physical Security Plan but rather in the licensee's

Behavior Observation Program documents. The Commission agrees in part with the second comment regarding the use of the annual supervisory review or interview, when applicable. All individuals must be subject to an annual supervisory review, and the Commission added the requirement that an individual be subject to a supervisory interview if his/her supervisor has not had frequent interaction with and observation of the individual throughout the review period. The Commission notes that not all supervisors have sufficient information about all of their employees due to current workforce practices and trends making close interaction between supervisors and their employees less common and difficult to achieve. Therefore, the Commission added the interview requirement to ensure that supervisors have an adequate basis to make an informed and reasoned opinion regarding an individual's behavior, trustworthiness, and reliability. Finally, the Commission agrees that the term "annual" should be used instead of "nominal 12-month" supervisor review as "annual" is the established component of industry practice.

The Commission received comments that the 5-year psychological reassessment requirements for individuals who are granted unescorted access or certified unescorted authorization in the proposed § 73.56(i)(1)(v)(A) deviates from current practice and imposes significant cost to the licensee with minimal benefits. The Commission agrees in part regarding the proposed 5-year psychological reassessments. The Commission agrees that requiring a psychological re-evaluation as part of the 5-year review for all individuals maintaining unescorted access or unescorted access authorization status will add significant and unnecessary costs, deviates from pre-existing requirements, and provides minimal benefits. Therefore, the Commission revised the final rule to limit the group of individuals who are subjected to 5-year psychological reassessments to those individuals who perform the job functions described in § 73.56(i)(1)(v)(B). The Commission believes these individuals should have a re-assessment on a periodic basis.

The Commission received comments that the requirement set forth in proposed § 73.56(i)(1)(v)(B), requiring the reviewing official to complete an evaluation of the criminal history update, credit history re-evaluation, psychological re-assessment, and the supervisory review within 30 calendar days of initiating any one of these elements, deviates from current practice as industry does not conduct these evaluations concurrently. The Commission agrees in part with the comment and revised § 73.56(i)(1)(v)(C) in the final rule to state that only the credit history review and the criminal history review are to be completed within 30 calendar days of each other to be consistent with current industry practice. Because the purpose of the re-evaluation is to provide a re-assessment based on a collective review of data at a point in time and because a credit history review and a criminal history review can be completed collectively within a small number of days, the Commission has retained this 30 calendar day requirement.

Section 73.56(k), Background Screeners. The Commission received comments that § 73.56(k)(2)(ii), regarding criminal history checks for access authorization program screening personnel, should be revised to allow licensees and applicants to use the criminal history check required by proposed § 73.56(d)(7) in lieu of a local criminal history review. The Commission agrees with the comments and revised the proposed rule text in the final rule to allow the flexibility of using either criminal history check process for individuals who are subject to the requirement because of a need for unescorted access or unescorted access authorization.

Section 73.56(m), Protection of Information. The Commission received comments that proposed § 73.56(m)(3), pertaining to providing information on denial or unfavorable termination of access determinations to authorized personnel, did not describe a means for licensees (1) to verify whether a representative who requests the reasons for denying its client's unescorted access is legitimate and (2) to protect the sources of the derogatory information. The Commission agrees with the received comments and revised § 73.56(m)(2) of the final rule to specify that representatives must be designated by the individual in writing and that personal

privacy information, including information pertaining to the source, may be redacted. The Commission concluded that these requirements are necessary to provide the regulatory framework to ensure the protection of personal information.

Section 73.56(n), Audits and Corrective Action. The Commission received comments that proposed § 73.56(n)(5), which would have required the audit team to include a person who is knowledgeable and practiced with meeting access authorization program performance objectives, is not appropriate for contractors or vendors. The commenters stated that the contractor or vendor audit team may not have such a person who is knowledgeable of and practiced with meeting authorization program performance objectives and requirements. The Commission disagrees. This requirement applies to licensees and applicants who are responsible for meeting the requirements of this section. The rule requires that licensees and applicants will perform audits of their access authorization program to include those program elements that are provided by contractors and vendors.

The Commission received comments on proposed § 73.56(n)(6) that it would not be consistent with appendix B to 10 CFR part 50 of this chapter, regarding who should receive the audit report. The Commission agrees and revised the final rule § 73.56(n)(6) to require that audit results be provided to senior management having responsibility in the area audited and to management responsible for the access authorization program to ensure proper disposition and oversight of issues identified during the conduct of audits.

**G. Section 73.58, Safety/Security Interface Requirements for Nuclear Power Reactors.**

The Commission did not make substantial changes to the final rule requirements for § 73.58. In response to comments, the Commission clarified the supporting section-by-section analysis for § 73.58. The principal concern expressed by stakeholders was that the proposed § 73.58 provisions appeared to require implementation of broad new programmatic

requirements, and that it did not appear that the NRC had sufficiently credited existing Commission required programs. It is not the intent of this new requirement to impose new programmatic requirements on licensees. If current programs and procedures are in place to enable the safety/security interface to be assessed and managed, the Commission expects that licensees would make maximum use of such programs. The Commission does not believe it is necessary to credit these existing programs in the rule. Instead, it intends to address the crediting of existing programs in supporting regulatory guidance. In response to public comment that expressed confusion as to the Commission's basis for imposing the new § 73.58 requirements, the Commission clarified the final rule section-by-section analysis for § 73.58 to indicate that the new requirement is being added to part 73 as a cost-justified, substantial, safety enhancement per § 50.109(a)(3) and in response to PRM-50-80.

**H. Appendix B to Part 73, General Criteria for Security Personnel.**

The Commission received comments on the proposed title of appendix B, section VI, which indicated that the title did not specify the applicability of this appendix to security personnel. The Commission agrees. The title of section VI of this appendix is revised to "Nuclear Power Reactor Training and Qualification Plan for Personnel Performing Security Program Duties" in the final rule to reflect the members of the security organization and other facility personnel that may be trained and qualified to perform security-related duties at an NRC-licensed nuclear power reactor facility.

Appendix B, Section VI.A.1. The Commission received comments on this paragraph that stated the proposed requirement could be broadly interpreted to apply to many varied licensee positions. The Commission agrees. The final rule is revised to clarify that the intent of this requirement is to ensure that all individuals who perform physical protection and/or contingency response duties within the security program meet the minimum training and qualification requirements for their assigned duties as specified within this appendix and the Commission-

approved training and qualification plan. The word “individuals” is used to capture members of the security organization as well as those facility personnel who are assigned to perform physical protection and/or contingency response duties within the security program. Facility personnel performing physical protection duties such as vehicle escort and materials search are included in the context of this paragraph and the paragraphs throughout this appendix where the word “individuals” is used, and is not preceded or followed by phrasing that specifically identifies members of the security organization. Facility personnel performing physical protection duties need only meet the minimum training and qualification requirements for the specific duty assigned in accordance with this appendix and the Commission-approved training and qualification plan. Where requirements of this appendix specifically apply to members of the security organization, the language explicitly identifies this applicability.

Appendix B, Section VI.A.3. The language in this paragraph, and paragraphs B.2.a(2), B.2.a(4), B.3.c, B.5.a, B.5.b, D.1.a, D.2.a, is revised from “members of the security organization” to “individuals.” This revision is necessary to include facility personnel who are not members of the security organization but have been trained and qualified in accordance with this appendix and the Commission-approved training and qualification plan and who are assigned to perform physical protection duties such as vehicle escort or material search.

Appendix B, Section VI.B.1.a(3). The language in this paragraph is revised to remove the phrase “an unarmed individual assigned to the security organization” as the applicability of this requirement is previously specified in section B.1.a.

Appendix B, Section VI.B.1.a(4). During development of the final regulations implementing the firearms background checks required under section 161A of the AEA (42 U.S.C. 2201a), the Commission recognized that the proposed suitability requirements for security personnel found in appendix B to part 73, criteria VI.B.1, were not inclusive of the list of disqualifying criteria found under the Gun Control Act of 1968 (GCA) (see 18 U.S.C. 922(g) and

(n)). The GCA mandates that it is unlawful for individuals who meet these disqualifying criteria to possess firearms or ammunition. During development of the guidelines required by section 161A of the EPAct (discussed previously in section I.D.(a)), the NRC discussed this issue with the U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosive (ATF) which has responsibility for regulatory oversight of this statute. The ATF's relevant regulation on these provisions is found in 27 CFR 478.32.

During these discussions, ATF advised the NRC that it interprets "any person" under 18 U.S.C. 922(d) very broadly and that the prohibition under this paragraph would apply to NRC licensees and certificate holders. Furthermore, the ATF indicated that this prohibition would apply to typical licensee or certificate holder security practices involving the temporary possession of firearms and ammunition. For example, instances in which a licensee issues firearms and ammunition to a security officer at the beginning of the officer's duty shift and the officer then returns the firearms and ammunition to the licensee at the end of the officer's duty shift would fall under the restrictions of 18 U.S.C. 922(d).

Consequently, the Commission has revised the language in Criteria VI.B.1 to remind licensees of their obligation to comply with this statutory requirement by adding a criterion to the licensee's employment suitability program for armed security officers. However, to account for the possibility that the law may change, or future laws may be enacted affecting this obligation, the final rule is written generically to maintain flexibility and reduce the potential need to revise this requirement in future rulemakings. The Commission is not imposing additional investigatory requirements on licensees. The Commission's intent is for licensees to consider information collected as a result of the individual's background investigation for identification of GCA disqualifying criteria.

In the proposed rule the Commission had set forth proposed requirements for a firearms background check under § 73.18. However, and as discussed elsewhere in this document, the

Commission is separating the provisions implementing section 161A of the EPAct 2005, into a separate rulemaking and intends to relocate the firearms background check provisions to § 73.19. Consequently, because that rule may not be issued before this rule or because a licensee may not otherwise be subject to the firearms background check requirement, this rule permits a licensee to satisfy the firearms background check requirement by comparing information obtained during their access authorization background investigation process with the disqualifying criteria under the GCA to evaluate whether an individual could be prohibited from possessing firearms and ammunition. The Commission notes that a final determination on whether an individual is, or is not, disqualified from possessing firearms and ammunition can be made via a Federal firearms background check or an applicable State firearms check. Furthermore, because this same issue also exists in criteria I.A.1 of appendix B for armed security personnel at other classes of NRC licensees and NRC certificate holders, the NRC also is making a conforming change in criteria I.A.1 of this appendix similar to that made to criteria VI.B.1 of this appendix.

Appendix B, Section VI.B.1.b. The Commission received comments on this proposed paragraph that stated this blanket addition of having a qualified training instructor document the qualifications of individuals assigned to perform physical protection and/or contingency response duties will create a huge administrative burden and add additional cost as processes overseen by other organizations (such as medical) would now require administration by a qualified training instructor. The NRC disagrees with this comment. The intent of this requirement is for the qualified training instructor to be responsible for the final documentation of each security critical task qualification as outlined in the Commission-approved training and qualification plan that is performed by individuals who are assigned physical protection and/or contingency response duties within the security program.

Appendix B, Section VI.B.2.a(1). The Commission received a comment recommending

that the phrase “of assigned security job duties and responsibilities” be added to the end of this provision in the final rule to allow the use of personnel in a limited duty position. The Commission agrees, and this paragraph is revised in the final rule to add the phrase “of assigned security duties and responsibilities” to the end of this provision to enable members of the security organization who are medically disqualified from performing contingency response duties or specific physical protection duties for a period of time to perform other physical protection duties that would not be affected by the medical disqualification.

Appendix B, Section VI.B.2.a(4). The Commission received comments on this proposed paragraph requesting further clarification as it appears that this requirement for armed and unarmed individuals who are assigned security duties and responsibilities identified in Commission-approved security plans and licensee protective strategy and implementing procedures (to meet the minimum physical requirements identified in this appendix) is more stringent than the existing requirement. The commenter specifically expressed the concern that personnel performing in day-to-day security operations but having little to no responsibility in an actual response to contingency events should not be required to meet an increased physical standard. The Commission disagrees with this comment. The physical standards associated with this requirement are identified in paragraphs B.2.b through B.2.f of this appendix within the final rule and reflect the basic physical requirements to ensure that an individual possesses the standard acuity levels associated with vision and hearing and that the individual does not have a medical condition that is detrimental to the individual's health or the performance of assigned duties. The standards identified in paragraphs B.2.b through B.2.f are applicable to all individuals who are assigned to perform physical protection and/or contingency response duties within the security program to include non-security organization personnel assigned to perform physical protection duties such as vehicle escort or material search.

Appendix B, Section VI.B.4.a. The Commission received comments on this proposed

paragraph which stated that this requirement for armed members of the security organization to be subject to a medical examination before participating in the physical fitness test is redundant to the requirement of paragraph B.2.a (2). The NRC agrees in part. The physical examination discussed in paragraph B.2.a (2) of this appendix may be used to fulfill this requirement. The rule requires that an individual's current health status be verified before engaging in the physical fitness test and that there is no existing medical condition that would be detrimental to the individual's health when placed under the physical stress induced by the physical fitness test. Scheduling the physical fitness test for each armed individual as soon as possible after the date of the physical examination required by paragraph B.2.a (2) provides the verification of the individual's current health status minimizes the possibility of the individual incurring a medical condition from the time of examination to the time that the physical fitness test is administered.

Appendix B, Section VI.B.4.b(4). The Commission received comments that this proposed requirement for a qualified training instructor to document the physical fitness qualifications of the armed members of the security organization should allow for the use of a trained medical professional to attest to the physical fitness qualification. The Commission disagrees with the comment. The licensed medical professional is required to conduct the medical examination before the physical fitness test being administered. The purpose of the examination is to verify that the individual's current health status is sufficient to engage in the physical exertion of the test without being detrimental to the individual's health. The licensed medical professional provides a certification of the individual's health before the test but is neither required to administer the physical fitness test nor to document or attest to the successful completion of the test. The rule requires that a qualified training instructor documents the successful completion of the physical fitness test in the individual's training record and that the documentation of the completed requirement be attested to by a security supervisor. The physical fitness test is a performance-based test that is designed to demonstrate an individual’s

physical ability to perform assigned security duties during a contingency event. The test consists of performing physical activities associated with contingency response duties that replicate site specific conditions that would be encountered in the contingency response environment.

Appendix B, Section VI.C.2. The Commission received comments requesting clarification of the scope of the on-the-job training requirements. The Commission agrees that the scope of this requirement should be clarified and has revised this paragraph to describe the implementation of on-the-job training. The requirement for on-the-job training is added to ensure that individuals assigned duties to implement the physical security plan and safeguards contingency plan possess practical hands-on knowledge, skills and abilities needed to perform their assigned duties. Beyond the on-the-job training for daily security program duties, the Commission requires an additional 40 hours of on-the-job training specific to response to contingency events. The rule requires that individuals (e.g. response team leaders, alarm station operators, armed responders, and armed security officers designated as a component of the protective strategy) assigned duties and responsibilities to implement the safeguards contingency plan complete a minimum of 40 hours of on-the-job training specifically related to the licensee's protective strategy to demonstrate their ability to apply the knowledge, skills, and abilities required to effectively perform assigned *contingency* duties and responsibilities *before* assuming those duties.

Appendix B, Section VI.C.3. The Commission received various comments requesting the relocation of the performance evaluation program requirements from the proposed part 73, appendix C, section II to part 73, appendix B, section VI. The Commission agrees, and the final rule is revised to include the performance evaluation program requirements that were contained in the proposed part 73, appendix C, section II.

Due to the merging of requirements within this section of this appendix, many requirements have changed location and are renumbered. The following proposed rule

paragraphs are removed from the performance evaluation program: the paragraph formerly identified as appendix C, section II.(l)(6)(iv): "Licensees shall ensure that scenarios used for required drills and exercises are not repeated within any twelve (12) month period for drills and three (3) years for exercises," is removed to provide licensees the flexibility to repeat scenarios in conducting tactical response drills and force-on-force exercises. The paragraph formerly identified as appendix B, section VI, C.3.b(2): "Tabletop exercises may be used to supplement tactical response drills and support force-on-force exercises to accomplish desired training goals and objectives," is more appropriate for regulatory guidance, therefore, is removed from this appendix.

The paragraph formerly identified as appendix C, paragraph (l)(5), stating that "members of the mock adversary force used for NRC-observed exercises shall be independent of both the security program management and personnel who have direct responsibility for implementation of the security program, including contractors, to avoid the possibility for a conflict of interest" has been deleted. As noted in the statements of consideration to the proposed rule, the intent of adding this provision to the rule was to address Section 651 of the EPAct 2005. (71 FR 62837) However, as noted above, the NRC does not normally subject itself to its own regulatory requirements codified in the Code of Federal Regulations. Section 651 imposes an obligation on the NRC to implement the requirements of Section 651, which it has done. Licensees are not responsible for this requirement. In light of this, the Commission has determined that removing this provision from the final rule is necessary and is therefore deleted.

Appendix B, Section VI.C.3(a). The Commission received a comment on this paragraph that stated that the requirements in appendix B, section VI, C.3 do not address Section 651 of the EPAct 2005, which requires that not less often than once every 3 years, the Commission shall conduct security evaluations (to include force-on-force exercises) at each licensed facility that is part of a class of licensed facilities, as the Commission considers to be appropriate, to

assess the ability of a private security force of a licensed facility to defend against any applicable design basis threat. Additionally, the commenter stated that this paragraph is not consistent with the current regulations, specifically § 73.46(b)(9) for Category I fuel cycle facilities which clearly states the requirement for a Commission role in the force-on-force exercise program. The Commission disagrees. Although the Commission has the discretion to issue regulations that govern its own practices (e.g. 10 CFR part 2), the Commission is not required to reflect a requirement in the form of its own regulations. If the NRC were required to implement an obligation in a particular way in a regulation, then direction would come from Congress in the authorizing statute. Unlike some other provisions of the EPAct 2005 (see, e.g., Section 170E requiring the NRC to conduct a rulemaking to revise the design basis threat), the EPAct 2005 did not require the Commission to implement the requirements of Section 651 by any particular method. In light of this, the Commission has the discretion to implement its statutory obligations as it sees fit.

The commenter references paragraph § 73.46(b)(9) (regarding force-on-force exercises for Category I strategic special nuclear material (SSNM) fuel cycle facilities) as an example of a regulation that imposes an obligation on the NRC to conduct force-on-force evaluations, and the commenter argues that the power reactor regulations should take a consistent approach. Section 73.46(b)(9), however, does not reflect the proposition claimed by the commenter. This provision requires that, during each 12-month period commencing on the anniversary of the date specified in § 73.46(i)(2)(ii) of this section, an exercise must be carried out at least every 4 months for each shift, one third of which are to be force-on-force and that during each of the 12-month periods, the NRC shall observe one of the force-on-force exercises. Thus, the regulation imposes an obligation on the licensee to organize and conduct a force-on-force exercise to meet the requirement and for the licensee to coordinate with the NRC who would "observe" one of those exercises. In contrast, the NRC is responsible for the conduct of force-

on-force exercises for power reactor licenses mandated by Section 651 of the EPAct 2005. That this requirement is not specifically reflected in a regulation is therefore not inconsistent with the requirements of § 73.46 and is consistent with the agency's long-established practices.

The Commission notes, however, that it has strictly complied with the requirements of Section 651. Since the enactment of Section 651, which added Section 170D of the AEA, the NRC has conducted over 80 force-on-force inspections at nuclear power plants. In addition, the NRC has submitted three annual reports to Congress describing the results of its security inspections, as required by Section 170D.e of the AEA. (See, e.g., the Commission's second annual report to Congress, available at http://www.nrc.gov/security/2006-report-to-congress.pdf). The Commission is, therefore, in full compliance with Section 170D of the AEA and does not see the need to codify requirements to impose an obligation on itself to meet this obligation.

Appendix B, Section VI.C.3.b. This proposed paragraph is revised to reflect the overall program scope that is the basis for its design, and the content of the necessary implementing procedures to conduct tactical response drills and force-on-force exercises. The periodicity requirement for the conduct of tactical response drills and force-on-force exercises is removed from this paragraph as it is specified in paragraph C.3.l(1) of this appendix.

Appendix B, Section VI.C.3.c. A commenter stated this section does not comply with the EPAct 2005 because this section does not state whether these exercises will be evaluated by NRC or even if the results of the drills will be required to be submitted to the NRC. As noted earlier, the Commission does not agree that it is appropriate to place a requirement on the NRC in this rule text. This proposed requirement (formerly paragraph C.3.b of this appendix) is renumbered and moved to the performance evaluation program section of this appendix. The text within this paragraph, as well as all of the other paragraphs within this appendix that include the specific text of "tactical response team drills and exercises," has been changed to "tactical response drills and force-on-force exercises" for accuracy and consistency of language.

Appendix B, Section VI.C.3.d. The proposed paragraph C.3.b(1) was renumbered and moved to the performance evaluation program section of this appendix. The Commission received comments that stated that, in the context of this paragraph, the rule language should focus on the scope of drills and exercises and not solely on the performance of individual participants. The Commission agrees and the final rule text was revised to address both the scope of conducting tactical response drills and force-on-force exercises as well as the importance of individual performance by the members of the security response organization.

Appendix B, Section VI.D.1.b. The Commission received comments which requested that this paragraph, pertaining to the annual written exam and performance demonstrations, be revised to be consistent with the current regulatory requirements. The Commission also received a comment recommending that the requirement for the annual written exam be relocated to paragraph F.7 of this appendix as it applies to armed security officers. The Commission agrees in part and has revised the requirement by replacing the phrase "annual written exam" with the phrase "written exams" to cover all written exams that may be administered to armed and unarmed individuals to demonstrate their proficiency. The requirement for the annual written exam is now addressed in paragraph D.1.b(3) and identifies the specific applicability of the annual written exam to armed members of the security organization.

Appendix B, Section VI.D.1.b(3). This paragraph is added to provide clarification on the specific applicability of the requirement for an annual written exam to be administered to armed members of the security organization.

Appendix B, Section VI.E.1.d. The Commission received comments requesting that the list of prescribed proficiency standards be revised so that it remains consistent with the standards outlined in the April 2003 training and qualification order (EA-03-039). The Commission disagrees that a revision is necessary. Most of the elements in this requirement

are retained from the pre-existing rule and reflect new elements that had been imposed by Commission orders. The additional items listed were not intended to be bound solely by the elements contained in the pre-existing list of order EA-03-039. The additions to the list reflect the Commission's expectation for training and the experience gained through nearly 30 years of security program inspections and observations. It is the Commission's view that these proficiency standards represent the minimal common firearms practices that must be followed to ensure the safe handling, operation, and appropriate training and qualification is achieved for weapons employed by a licensee. Nonetheless, this requirement has been revised to reflect accurate language consistent to what is used in the firearms community for the performance elements identified.

Appendix B, Section VI.F.1.c. The Commission received comments that recommended deleting the proposed requirement for individuals to be requalified annually as it is duplicative of the requirement stated in paragraph F.5 (proposed rule paragraph F.6). The Commission agrees and this requirement is removed in the final rule.

Appendix B, Section VI.F.2. The proposed rule paragraph F.2 is removed as the requirements for firearms qualification courses are clearly identified in paragraphs F.2, F.3, and F.4 (proposed rule paragraphs F.3, F.4, and F.5) of this appendix.

Appendix B, Section VI.F.3.a. This requirement has been renumbered due to the removal of other requirements under this paragraph. The Commission received comments on proposed rule paragraph F.4.a stating that the requirement for daytime shotgun proficiency has increased by 20 percent above the current requirement with no rationale provided. The Commission disagrees. The shotgun qualification score was upgraded from 50 percent in the current rule to a score of 70 percent to demonstrate an acceptable level of proficiency which is now reflected in this appendix. The Commission found 70 percent to be a professionally accepted minimum qualification score for daytime shotgun proficiency in the firearms training

community (local, State, and Federal law enforcement, National Rifle Association (NRA), International Association of Law Enforcement Firearms Instructors (IALEFI), etc.).

Appendix B, Section VI.F.3.b. This requirement has been renumbered from proposed rule paragraph F.4.b due to the removal of other requirements under this paragraph. The Commission received comments that stated nighttime shotgun proficiency has increased by 20 percent above the current requirement with no rationale provided. The Commission disagrees. The Commission found 70 percent to be a professionally accepted minimum qualification score for nighttime shotgun proficiency in the firearms training community (local, State, and Federal law enforcement, NRA, IALEFI, etc.). The "night fire" requirement is upgraded from being an element of familiarization fire in the current rule to a qualification requirement in the final rule. This upgrade is necessary to ensure armed members of the security organization possess and maintain a standard level of proficiency during nighttime conditions. A score of 70 percent for handgun and shotgun and 80 percent for the semi-automatic rifle and/or machine gun must be achieved to demonstrate an acceptable level of proficiency.

Appendix B, Section VI.F.5. The NRC received comments on proposed rule paragraphs F.5.a (2), F.5.b (2), F.5.c (2), and F.5.d (2) that recommended deleting these requirements as they are duplicative of the requirements in paragraphs F.3.a, b, and c (formerly paragraphs F.4.a, b, and c). The Commission agrees that these requirements are duplicative and has therefore removed them from the final rule. The minimum qualification score for these weapons are stated in the re-numbered paragraphs F.3.a and F.3.b of this appendix.

Appendix B, Section VI.F.5.a. The Commission received a comment on proposed rule paragraph F.6.a that recommended adding the phrase "and the results documented and retained as a record" to the end of the provision. The Commission agrees and this requirement is revised to include the recommended phrase. The rule requires licensees to document the

successful completion of qualifications for each weapon system fired and that records of qualifications be maintained.

Appendix B, Section VI.G.2.b. The Commission received a comment stating that the rule should not require that security officers carry body armor with them but rather that body armor be readily available should the security officers choose to wear it. The commenter also noted that every security officer is already required to have access to body armor. The commenter, therefore, suggested that the rule be revised to permit the pre-staging of body armor at assigned response positions as appropriate. The commenter also noted that duress alarms are not personal equipment required for security officers and should not be listed as such. The Commission agrees with the commenter and has revised this paragraph in the final rule to clarify the specific applicability of the required equipment listing to those armed security personnel who are responsible for the implementation of the safeguards contingency plan, protective strategy, and associated implementing procedures. This revision permits a licensee to pre-stage equipment (such as body armor) at designated locations consistent with their protective strategy. The required equipment listing under this paragraph is also revised to remove "(4) Duress alarms" as this piece of equipment is not personal equipment associated with the specific duties of armed security personnel. It is added, however, to § G.2.c as an optional piece of equipment that may be made available for use in accordance with the protective strategy and implementing procedures.

Appendix B, Section VI.G.2.c. The Commission received a comment that the listing of personal equipment should not prescriptively identify particular pieces of equipment as either optional or required but rather the rule should permit licensees to designate required personal equipment based on individual protective strategy requirements. The commenter recommended that the term "as appropriate" be inserted after the text "should provide" within the paragraph. The Commission agrees in part, and this paragraph is revised in the final rule to include the

recommended phrase to further clarify the suggested employment and distribution of the identified equipment that should be provided in accordance with licensee policy and implementing procedures. The equipment listing under this paragraph is revised to include "duress alarms" as the equipment identified in this listing is based upon what may be deemed by the licensee as appropriate to fulfill specific physical protection and/or contingency response duties as well as provide enhanced capabilities to the security organization during day-to-day security operations and contingency events.

Appendix B, Section VI.G.3.a. The NRC received a comment that the requirement for armorer certification is new and not well-defined by the proposed rule. The commenter believes that the requirement that the armorer be certified is unnecessary because it limits licensee flexibility to use experienced but uncertified personnel. The Commission disagrees. The rule requires that only those individuals who are certified by the weapons manufacturer or a contractor working on behalf of the manufacturer shall be used to perform maintenance and repair of licensee firearms. Licensees may use a manufacturer's armorer and certification process or use a contractor certified by the manufacturer as an armorer to perform maintenance and repair of licensee firearms. The proposed language of this requirement is maintained in the final rule text.

**H. Appendix C to Part 73, Licensee Safeguards Contingency Plans.**

General. The Commission received comments on this appendix that the proposed changes would expand focus of the safeguards contingency plan (SCP) by requiring specifics on non-security response efforts to prevent significant core damage. In addition, the commenters stated that the level of detail that would be required in the SCP would be inappropriately increased. The Commission agrees in part. It is the Commission's intent that licensee's SCP focus on the predetermined actions of the site security force, and the final rule has been revised to clarify this focus. The intent is not to incorporate other site emergency plans into the SCP but

to ensure that the licensee has considered these other plans to avoid potential conflict. To accomplish this, the NRC retained rule language in a format similar to the current regulation, included requirements similar to those that had been imposed by the Commission orders, reorganized the requirements, and modified the language for a more concise understanding.

Appendix C, Section II.B Contents of the Plan. The Commission received comments that the proposed appendix C inappropriately included a licensee's entire integrated response for all postulated events including those beyond the DBT. The commenters were also concerned that portions of these requirements were not security related and, therefore, should not be included in the security rule. The Commission agrees in part with these comments and has revised the final rule accordingly. Appendix C, section II has been revised to more clearly reflect what the Commission expects to be included in a licensee's SCP. The following proposed rule categories of information have been moved to the licensee's planning basis: (5) "Primary Security Functions," (6) "Response Capabilities," and (7) "Protective Strategy."

The proposed rule category of information (8) "Integrated Response Plan" is also removed from this appendix. The requirements associated with this paragraph have been removed, modified, and/or relocated to other applicable areas within this appendix to reduce confusion related to the redundancy and duplication of information. In addition, the proposed rule category of information (9) "Threat Warning System" is removed from this appendix and included in 10 CFR 73.55 (k)(10). The proposed rule category of information (9) requirement regarding 'imminent threat' is relocated to new 10 CFR 50.54(hh)(1).

The Commission received comments that the requirements of the performance evaluation program be moved to part 73, appendix B. As explained earlier, the Commission agrees. The proposed rule category of information (10) "Performance Evaluation Program" is removed from this appendix in its entirety and has been incorporated in part 73, appendix B, as these requirements describe the development and implementation of a training program for the

security force in response to contingency events.

## IV. Section-by-Section Analysis.

### A. Introduction.

The purpose of this section is to identify what sections are being affected by this final rulemaking and to provide explanations of the purpose, scope, and intent of each section.

### B. Section 50.34, Contents of Construction Permit and Operating License Applications; Technical Information.

Paragraph (c) of § 50.34 is revised to require applicants for an operating license to submit a training and qualification plan (in accordance with appendix B to part 73) and a cyber security plan (in accordance with the criteria in § 73.54). These plans are in addition to the licensee's physical security plan. Paragraph (c) is revised such that the submittal requirements for applicants for licensees that are subject to §§ 73.50 and 73.60 remain unchanged.

Paragraph (d) of § 50.34 is revised to require applicants for an operating license to submit a safeguards contingency plan in accordance with section II of appendix C to part 73. Section II of appendix C is revised to contain the requirements limited to power reactor licensees. Additionally, paragraph (d) is revised so that the safeguards contingency plan submittal requirements for applicants for licenses that are subject to §§ 73.50 and 73.60 remain unchanged by requiring that these applicants follow section I of appendix C to part 73.

Paragraph (e) of § 50.34 is revised to require the cyber security plan, which is a new plan required by this rulemaking and which contains Safeguards Information, to be protected against unauthorized disclosure consistent with § 73.21.

Paragraph (i) is added to § 50.34 to require submittal of a description and plans for implementation of the guidance and strategies intended to maintain or restore core cooling, containment, and spent fuel pool cooling capabilities under the circumstances associated with

the loss of large areas of the plant due to explosions or fire as required by § 50.54(hh)(2). Regarding the requirements of § 50.54(hh)(2), the NRC views the mitigative strategies as similar to those operational programs for which a description of the program is provided as part of the license application and that will be implemented before plant operation. The Commission plans to review the program description provided in the application as part of the licensing process and perform subsequent inspections of procedures and plant hardware to verify implementation. Because the Commission finds that the most effective approach is for the mitigative strategies, at least at the programmatic level, to be developed before construction and reviewed and approved during licensing, a requirement for information has been added to §§ 50.34 and 52.80.

**C. Section 50.54, Conditions of Licenses.**

Section 50.54(p)(1) is revised to add the cyber security plan to the list of plans for which the plan changes need to be controlled by § 50.54(p).

**D. Section 50.54(hh), Mitigative Strategies and Response Procedures for Potential or Actual Aircraft Attacks.**

The mitigative strategies and response procedure requirements for potential or actual aircraft attacks are located in new § 50.54(hh) so that these requirements are a condition of an operating or combined license. This approach was chosen to ensure consistency with the method by which the 2002 ICM order B.5.b mitigative strategies requirements have been implemented for currently operating reactors. (See Orders Modifying Licenses, 71 FR 36554; June 27, 2006).

Section 50.54(hh)(1) establishes the necessary regulatory framework and clarifies current expectations to facilitate consistent application of Commission requirements for preparatory actions to be taken in the event of a potential aircraft threat to a nuclear power reactor facility. Because aircraft threats are significant, rapidly evolving events and because licensees may only receive threat notifications a short time before potential onsite impacts, the

NRC has determined that it is not prudent for licensees to attempt to identify and accomplish *ad hoc* mitigative actions in the midst of such circumstances and employing a reactive approach would significantly limit the effectiveness of onsite and offsite responses. To cope effectively with potential aircraft threats, the rule requires licensees to develop specific procedures, whether in a single procedure or among several procedures, that describe the pre-identified actions licensees intend to take when they are provided with pre-event notification. These pre-event preparations provide the most effective responses possible to aircraft threats and demonstrate systematic onsite and offsite planning, coordination, communication, and testing.

To the extent possible, the rule requires licensees to develop, implement, and maintain procedures for verifying the authenticity of aircraft threat notifications to avoid taking actions in response to hoaxes that may adversely impact licensees or the health and safety of the public. Depending on the source of a threat notification, licensees may or may not be able to establish contact with appropriate entities to confirm the accuracy of the threat information received. Consequently, if the threat information is not received from the NRC Headquarters Operations Center, licensees are required to at least contact the NRC Headquarters Operations Center for assistance with verifying callers' identities or the veracity of threat information.

The national protocol for dealing with aircraft threats is designed to be proactive with respect to threat identifications and notifications. However, threat information sources may not be able to identify specific targets, and given the dynamic nature of potential aircraft threats, any associated notifications to licensees may necessarily be reactive in nature. Additionally, licensees must rely on sources which are external to their control rooms for potential aircraft threat notifications and updates when available. As a result, the rule requires licensees to develop, implement, and maintain procedures for the maintenance of continuous communication with threat notification sources because it is imperative that licensees establish and maintain this capability throughout the duration of the pre-event notification period. With such a capability,

licensees will be able to receive accurate and timely threat information upon which to base decisions concerning the most effective actions that need to be taken. For example, licensees would be aware that they may be able to cease mitigative actions if it is determined a threat no longer exists, or licensees may accelerate their protective actions if the threat notification sources relate the aircraft may impact sooner than originally projected. The local, regional or national FAA offices; NORAD; law enforcement organizations; and the NRC Headquarters Operations Center are examples of threat notification sources with which licensees would be required to maintain a continuous communication capability. If a licensee encounters a situation where multiple entities are providing the same threat information (e.g., FAA, NORAD and NRC Headquarters Operations Center), the licensee would only be required to maintain continuous communication with the NRC Headquarters Operations Center. The goal is to communicate pertinent information to licensees and not to unnecessarily burden their personnel with redundant requirements.

The rule also requires that licensees develop, implement, and maintain procedures for contacting all onsite personnel and appropriate offsite response organizations (e.g., fire departments, ambulance services, emergency operations centers) in a timely manner following the receipt of potential aircraft threat notifications. These notifications ensure that onsite personnel have as much time as possible to execute established procedures and provide offsite response organizations the opportunity to perform the following:

- Initiate, where possible, mutual aid assistance agreements based on the perceived threat;
- Commence the near-site mustering of offsite fire-fighting and medical assistance for sites where these organizations are not proximately located; or
- Mobilize personnel for volunteer organizations or hospital staffs when appropriate.

Licensees are expected to provide periodic updates to offsite response organizations

during the pre-event notification period as appropriate. During the pre-event notification period, the rule requires licensees to develop procedures to continuously assess plant conditions and take effective actions to mitigate the consequences of an aircraft impact. Examples include maximizing makeup water source inventories, isolating appropriate plant areas and systems, ceasing fuel-handling operations and equipment testing, starting appropriate electrical generation equipment, and charging fire-service piping headers. By taking these actions, licensees can better posture their sites to minimize the potential public health and safety effects of an aircraft crash at their facilities.

The rule also requires licensees to develop, implement, and maintain procedures for making site-specific determinations of the amount of lighting required to be extinguished, if any, to prevent or reduce visual discrimination of sites relative to their immediate surroundings and distinction of individual buildings within protected areas. For example, it may make sense to turn off all the lights at an isolated site but not for a site situated in an industrial area where ambient lighting from surrounding industries is sufficient for target discrimination. Licensees are expected to use centralized lighting controls or develop prioritized routes that allow personnel to turn off different sets of lights depending on available time when appropriate.

The safety of licensee personnel and contractors is paramount to the successful response and implementation of mitigative measures after an onsite aircraft impact. To the maximum extent possible after an imminent aircraft threat notification, the rule also requires licensees to develop, implement, and maintain procedures for dispersing appropriate personnel and equipment (e.g., survey vehicles and emergency kits) to locations throughout their sites. Such actions will increase the chance that critical personnel and equipment will be available to address the consequences of an onsite aircraft impact and reduce the need to make improvised decisions during the pre-event notification period. The decision whether to shelter the remaining personnel in-place or evacuate them in response to an imminent aircraft threat should be based

on the physical layout of the site and the time available to conduct an effective evacuation. It is expected that licensees will conduct an analysis and develop a decision-making tool for use by shift operations personnel to assist them in determining the appropriate onsite protective action for site personnel for various warning times and site population conditions (e.g., normal hours, off normal hours, and outages). This decision-making tool shall be incorporated into appropriate site procedures. It is expected that this tool will be routinely used in drills and exercises and that any deficiencies or weaknesses identified will be corrected in accordance with § 50.47(b)(14) and appendix E to part 50, section IV.F.2.g. Depending upon the methodology used to determine evacuation times, it may not be necessary for a licensee to suspend security measures under §§ 50.54(x) or 73.55(p), as applicable. Licensees are required to develop procedures to facilitate the rapid entry of appropriate onsite personnel as well as offsite responders into their protected areas to deal with the consequences of an aircraft impact.

Because the most well-considered plans and procedures do not guarantee that critical on-shift personnel will survive an aircraft impact, the rule requires licensees to develop, implement, and maintain procedures for an effective recall process for appropriate off-shift personnel. Those procedures shall describe the licensee's process for initiating off-shift recalls during the pre-event notification period and for directing responding licensee personnel to pre-identified assembly areas outside the site protected areas. When possible, the assembly area locations should be coordinated with offsite response organizations to facilitate offsite response plans and to ensure that off-shift licensee personnel will not be delayed access to the site onsite when needed.

Section 50.54(hh)(2) requires licensees to develop guidance and strategies for addressing the loss of large areas of the plant due to explosions or fires from a beyond-design basis event through the use of readily available resources and by identifying potential practicable areas for the use of beyond-readily-available resources. These strategies are to address a

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

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

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

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

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

consideration of water spray scrubbing and dose to onsite responders.

The Commission considered specifically including these 14 strategies in § 50.54(hh)(2). However, the Commission decided that the more general performance-based language in § 50.54(hh)(2) was a better approach to account for future reactor facility designs that may contain features that preclude the need for some of these strategies. New reactor licensees are required to employ the same strategies as current reactor licensees to address core cooling, spent fuel pool cooling, and containment integrity. The mitigative strategies employed by new reactors as required by this rule would also need to account for, as appropriate, the specific features of the plant design, or any design changes made as a result of an aircraft assessment that would be performed in accordance with the proposed Aircraft Impact Assessment rule (72 FR 56287; October 3, 2007).

Section 50.54(hh) is applicable to both current reactor licensees and new applicants for and holders of reactor operating licenses under either part 50 or part 52. Current reactor licensees have already developed and implemented procedures that comply with the § 50.54(hh)(2) requirements, and do not require any additional action to comply with these rule provisions. New applicants for, and new holders of, operating licenses under part 50 and combined licenses under part 52 are required to develop and implement procedures that employ mitigative strategies similar to those now employed by current licensees to maintain or restore core cooling, containment, and spent fuel pool cooling capabilities under the circumstances associated with loss of large areas of the plant due to explosions or fire. The requirements described in § 50.54(hh) relate to the development of procedures for addressing certain events that are the cause of large fires and explosions that affect a substantial portion of the nuclear power plant and are not limited or directly linked to an aircraft impact. The rule contemplates that the initiating event for such larges fires and explosions could be any number of beyond-design basis events. In addition, the Commission regards § 50.54(hh) as necessary for

reasonable assurance of adequate protection to public health and safety and common defense and security; this is consistent with the NRC's designation of the orders on which § 50.54(hh) is based as being necessary for reasonable assurance of adequate protection.

As discussed previously, the Commission has proposed in a separate rulemaking to require designers of new nuclear power plants (e.g., applicants for standard design certification under part 52, and applicants for combined licenses under part 52) to conduct an assessment of the effects of the impact of a large commercial aircraft on a nuclear power plant. Based upon the insights gained from this assessment, the applicant will be expected to include a description and evaluation of design features and functional capabilities to avoid or mitigate, to the extent practical and with reduced reliance upon operator actions, the effects of the aircraft impact. New reactor applicants would be subject to both the requirements of the aircraft impact rule and the requirements § 50.54(hh). The overall objective of the Commission with both rulemakings is to enhance a nuclear power plant's capabilities to withstand the effects of a large fire or explosion, whether caused by an aircraft impact or other event, from the standpoints of both design and operation. The impact of a large aircraft on the nuclear power plant is regarded as a beyond-design basis event. In light of the Commission's view that effective mitigation of the effects of events causing large fires and explosions (including the impact of a large commercial aircraft) should be provided through operational actions, the Commission believes that the mitigation of the effects of such impacts through design should be regarded as a safety enhancement which is not necessary for adequate protection. Therefore, the aircraft impact rule – unlike the § 50.54(hh) – is regarded as a safety enhancement which is not necessary for adequate protection.

The Commission regards the two rulemakings to be complementary in scope and objectives. The aircraft impact rule will focus on enhancing the design of future nuclear power plants to withstand large commercial aircraft impacts, with reduced reliance on human activities

(including operator actions). Section 50.54(hh)(2) focuses on ensuring that the nuclear power plant's licensees will be able to implement effective mitigative measures for large fires and explosions including (but not explicitly limited to) those caused by the impacts of large commercial aircraft. Thus, these revisions to the Commission's regulatory framework for future nuclear power plants provide more regulatory certainty, stability, and increased public confidence.

Section 50.54(hh) requirements do not apply to decommissioning facilities for which the certifications required under § 50.82(a)(1) or § 52.110(a)(1) have been submitted. The NRC believes that it is inappropriate that § 50.54(hh) should apply to a permanently shutdown defueled reactor where the fuel was removed from the site or moved to an ISFSI. The Commission notes that the § 50.54(hh) do not apply to any current decommissioning facilities that have already satisfied the § 50.82(a) requirements.

The Commission issued guidance (Safeguards Information) to current reactor licensees on February 25, 2005, and additionally endorsed NEI 06-12, Revision 2, by letter dated December 22, 2006, as an acceptable method for current reactor licensees to comply with the mitigative strategies requirement. These two sources of guidance provide an acceptable means for developing and implementing the mitigative strategies. The Commission is currently developing a draft regulatory guide that consolidates this guidance and addresses new reactor designs.

**E. Section 52.79, Contents of Applications; Technical Information in Final Safety Analysis Report.**

Section 52.79(a)(36) is revised to require the cyber security plan, developed in accordance with the criteria set forth in § 73.54, to be included amongst the security plans that are required to be included in the final safety analysis report for a combined license under part 52. In addition, the cyber security plan is added to the list of plans which must be handled

as Safeguards Information in accordance with § 73.21.

**F. Section 52.80, Contents of Applications; Additional Technical Information.**

Section 52.80(d) is added to § 52.80 to require a combined license applicant to submit a description and plans for implementation of the guidance and strategies intended to maintain or restore core cooling, containment, and spent fuel pool cooling capabilities under the circumstances associated with the loss of large areas of the plant due to explosions or fire as required by § 50.54(hh)(2) of this chapter. The Commission views the mitigative strategies required by § 50.54(hh)(2) as similar to those operational programs for which a description of the program is provided as part of the combined license application and subsequently implemented before plant operation. The Commission reviews the program description provided in the application as part of the licensing process and performs subsequent inspections of procedures and plant hardware to verify implementation.

**G. Section 72.212, Conditions of General License Issued Under § 72.210.**

Conforming changes were made to § 72.212 to reference the appropriate revised paragraph designations in § 73.55. No change to the substantive requirements of this section is intended. Conforming changes were made to preserve the current requirements for general licenses issued per § 72.210 for the storage of spent fuel in an ISFSI. The Commission has initiated a separate rulemaking to revise the requirements for the security of ISFSIs and thus prefers to maintain the current regulatory structure until that rulemaking is completed. Section 72.212(b)(5) requires that spent fuel stored in an ISFSI be protected against the design basis threat of radiological sabotage with conditions and exceptions. The changes made to § 72.212 are intended to preserve those conditions and exceptions since these ISFSI licensees are not the subject of the rulemaking. Specifically, § 72.212(b)(5)(ii) is revised to reference § 73.55(e) because § 73.55(e) provides the protected area criteria, within which the spent fuel must be stored, while preserving the exception that spent fuel is not required to be within a

separate vital area.

Section 72.212(b)(5)(iii) is revised to reference § 73.55(h) because § 73.55(h) provides the personnel search criteria for § 72.212. Section 72.212 provides an exception allowing a physical pat-down search of persons to be performed in lieu of the use of firearms and explosives detection equipment. Section 72.212(b)(5)(iv) is revised to reference § 73.55(i)(3) since § 73.55(i)(3) provides the intrusion detection and assessment requirements for which § 72.212 provides an exception allowing a guard or watchman on patrol to provide this observational capability. Section 72.212(b)(5)(v) is revised to exempt ISFSI licensees from the requirements in § 73.55 to interdict and neutralize threats preserving this exception. Due to the restructuring of § 73.55, a specific reference to a paragraph in § 73.55 was no longer possible, and a more general exception was written into § 72.212. The Commission intends for the same exception to continue.

**H. Section 73.8, Information Collection Requirements: OMB Approval.**

Section 73.8 is revised to add § 73.54 and § 73.58 to the list of part 73 sections, which contain collection requirements that have been approved by the Office of Management and Budget.

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

This new section describes the requirements for nuclear power plant licensees to establish a cyber security program.

Section 73.54, General**.** This section requires current nuclear power plant licensees to submit a cyber security plan within 180 days of the effective date of the rule for NRC review and approval. The cyber security plan must be submitted to the NRC as a license amendment pursuant to § 50.90. Current applicants for an operating license or combined license who have submitted their applications to the NRC prior to the effective date of this rule are required to

amend their applications to include a cyber security plan consistent with this rule.

Section 73.54(a), Protection**.** This paragraph establishes the regulatory framework and requirements for the cyber security program in meeting the requirement for protection against the design basis threat of cyber attack identified in § 73.1. This paragraph has been expanded from the proposed rule to provide a more detailed list of the types of systems and networks that are intended to be protected.

Section 73.54(b), Analysis of Digital Computer and Communication Systems and Networks. This paragraph establishes requirements for an analysis. The rule requires that each licensee will analyze the digital computer and communication systems and networks in use at their facility to identify those assets that require protection and that the licensee's cyber security program will include measures for the protection of the digital computer and communication systems and networks identified by the licensee through the required analysis. Cyber security, like physical security, focuses on the protection of equipment, systems, and networks against attacks by those individuals or organizations that would seek to cause harm, damage, or adversely affect the functions performed by such equipment, systems, and networks. Cyber security and physical security programs are intrinsically linked and must be integrated to satisfy the physical protection program design criteria of § 73.55(b). The Commission recognizes that a uniquely independent technical expertise and knowledge is required to effectively implement the cyber security program, and therefore, the specific training and qualification requirements for the program must focus on ensuring that the personnel who implement the cyber security program are trained, qualified, and equipped to perform their unique duties and responsibilities.

Section 73.54(c), Cyber Security Program**.** This paragraph describes the design components of the cyber security program including controls, prevention, defense-in-depth, and system functionality. The cyber security program must be designed to implement security controls for protected digital assets; apply and maintain defense-in-depth protective strategies to

ensure the capability to detect, respond, and recover from cyber attacks; and ensure the functions of protected digital assets are not adversely impacted due to cyber attacks. With regard to § 73.54(c)(4), the NRC requires that the cyber security program to be designed to ensure that the intended function of the assets identified by § 73.54(a)(1) and the analysis required by § 73.54(b)(1) are maintained.

With regard to § 73.54(c)(2), defense-in-depth for digital computer and communication systems and networks includes technical and administrative controls that are integrated and used to mitigate threats from identified risks. The need to back up data as part of a defense-in-depth program is dependent upon the nature of the data relative to its use within the facility or system.

Defense-in-depth is achieved when (1) a layered defensive model exists that allows for detection and containment of non-authorized activities occurring within each layer, (2) each defensive layer is protected from adjacent layers, (3) protection mechanisms used for isolation between layers employ diverse technologies to mitigate common cause failures, (4) the design and configuration of the security architecture and associated countermeasures creates the capability to sufficiently delay the advance of an adversary in order for preplanned response actions to occur, (5) no single points of failure exist within the security strategy or design that would render the entire security solution invalid or ineffective, and (6) effective disaster recovery capabilities exist for protected systems.

The Commission's intent for a licensee's cyber security program is that a licensee or applicant implements operational elements to address the requirements of this rule but not necessarily address such requirements through the design of its facility. However, as with other elements of a licensee's physical security program, an applicant or licensee could consider how these requirements could be addressed through the design of its facility, to the extent practicable, but this is not required by the rule.

Section 73.54(d), Cyber-Related Training, Risk and Modification Management. This paragraph requires licensees to develop, implement, and maintain supporting programs within the cyber security program. The Commission requires licensees to perform an analysis as identified in § 73.54(b)(1) for any newly installed digital computer and communication systems and network equipment whether the new equipment is stand-alone or is installed to replace outdated equipment.

To ensure that the measures used to protect digital computer and communication systems and networks remain effective and continue to meet high assurance expectations, the licensee's cyber security program must evaluate and manage cyber risks. Licensees must evaluate changes to systems and networks when modifications are proposed for previously assessed systems and new technology-related vulnerabilities not previously analyzed in the original baseline or periodic assessments that would act to reduce the cyber security environment of the system are identified.

Section 73.54(e), Cyber Security Plan**.** This paragraph establishes the requirements for a written cyber security plan that outlines the licensee's implementation of their program to include incident response and recovery, detection, response, mitigation, vulnerabilities, and restoration. The plan must describe how the Commission requirements of this section are implemented and must account for site-specific conditions that affect implementation. Applicants for combined license under part 52 of this chapter should have sufficient information available to prepare and submit a plan as required by § 52.79. Such plans will likely require updates and revisions in accordance with § 50.54(p) as digital networks and systems are better defined during a plant's specific design and construction. The rule requires that the cyber security incident response and recovery measures will be part of the cyber security plan.

Section 73.54(f), Policies and Procedures. This paragraph establishes requirements for licensees to have and maintain written policies and procedures for the implementation of the

cyber security plan. The Commission does not intend for licensees to submit policies, implementing procedures, site-specific analysis, and other supporting technical information used by the licensee in development of their cyber security plan; however, such information must be made available upon request by an authorized representative of the NRC.

Section 73.54(g), Reviews**.** This paragraph establishes the licensee review requirements for the cyber security program. The rule requires that the cyber security program be reviewed by the licensee on a periodic basis in accordance with § 73.55(m).

Section 73.54(h), Records. This paragraph establishes record retention requirements for the cyber security program. The rule requires that each licensee will retain the technical information associated with the assets identified by § 73.54(b)(1) pertinent to compliance with § 73.54.

**J. Section 73.55, Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage.**

Section 73.55(a), Introduction**.** This paragraph outlines the implementation, plans, program, scope and applicability of this section. The rule requires that each licensee shall evaluate the security plan changes needed to comply with the amended requirements of the final rule. Licensees are expected to make any changes necessary to comply with the final rule within 180 days. It is up to the licensee to determine the appropriate mechanism to make those changes whether it be as a change under § 50.54(p) or as a license amendment pursuant to § 50.90. As noted earlier, it is the Commission's view that current licensees are largely already in compliance with the requirements in this rule, and any changes that would be necessitated by this final rule would not decrease the effectiveness of current licensee security plans, so in most instances a change under § 50.54(p) would be appropriate. However, the Commission also acknowledges that, based on site-specific conditions, a limited number of plan changes might require Commission review and approval before implementation. In such instances, licensees

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

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

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

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

specific analysis that accounts for site conditions and utilizes the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures. The physical protection program is supported by the access authorization, cyber security, and insider mitigation programs to meet the performance object of this section. The effectiveness of the physical protection program specific to the licensee protective strategy is measured through implementation of the performance evaluation program.

Section 73.55(c), Security plans. This paragraph outlines the requirements for, contents of, and protection of security plans and implementing procedures. The primary focus of the security plans is to describe how the licensee will satisfy Commission requirements to include how site-specific conditions affect the measures needed at each site to ensure that the physical protection program is effective. Security plans include the physical security plan, training and qualification plan, safeguards contingency plan, and cyber security plan. The cyber security plan is subject to the same review and approval process as the physical security plan, training and qualification plan, and safeguards contingency plan.

Section 73.55(d), Security Organization**.** This paragraph outlines the requirements for the composition, equipping, and training of the security organization. The intent is that the security organization will focus upon the effective implementation of the physical protection program. Individuals assigned to perform physical protection or contingency response duties must be trained, equipped, and qualified in accordance with appendix B to perform those assigned duties and responsibilities whether that individual is a member of the security organization or not. The rule requires that facility personnel, who are not members of the security organization, will be trained and qualified for the specific physical protection duties that they are assigned which includes possessing the knowledge, skills, abilities, and the minimum physical qualifications.

Section 73.55(e), Physical Barriers. This paragraph outlines the generic and specific

requirements for the design, construction, placement, and function of physical barriers. Physical barriers are used to fulfill many functions within the physical protection program, and therefore, each physical barrier must be designed and constructed to serve its predetermined function within the physical protection program. The rule requires that each licensee will analyze site-specific conditions to determine the specific use, type, function, construction, location, and placement of physical barriers needed for the implementation of the physical protection program. This paragraph also describes the requirements to maintain the integrity of physical barriers through the implementation of maintenance and observation measures.

Section 73.55(f), Target Sets. This paragraph provides requirements for the development, documentation, and periodic re-evaluation of target sets. Target sets are a minimum combination of equipment or operator actions which, if 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 destruction) or a loss of coolant and exposure of spent fuel barring extraordinary actions by plant operators. Credit for operator actions will be given only if the following criteria are met: (1) sufficient time is available to implement these actions, (2) environmental conditions allow access where needed, (3) adversary interference is precluded, (4) any equipment needed to complete these actions is available and ready for use, (5) approved procedures exist which have entering conditions outside of severe accident mitigation guidelines (SAMG) or equivalent, and (6) training is conducted on the existing procedures under conditions similar to the scenario assumed. This rule requires each licensee to implement a process for the oversight of target set equipment, systems, and configurations using existing processes. This ensures that changes made to the configuration of target set equipment and modes of operation are considered in the licensee's protective strategy. Target set requirements include consideration of the effects of cyber attacks and is consistent with Commission requirements for protection against the design basis threat of

radiological sabotage stated in § 73.1.

Section 73.55(g), Access Controls**.** This paragraph outlines the requirements regarding access control systems, devices, processes, and procedures for personnel, vehicles, and materials during normal and emergency conditions. Access controls relative to the owner controlled area, protected area, and vital areas are specifically addressed within this paragraph including visitor and escort requirements. The rule requires that the licensee will ensure that all access controls are performing as intended and have not been compromised such that no person, vehicle, or material is able to gain unauthorized access beyond a barrier.

With regard to escorts, the rule requires that all escorts will be trained to perform escort duties and that this training may be accomplished through existing processes, such as the General Employee Training (personnel escort) and/or the security Training and Qualification Plan (vehicle escorts). Personnel escorts are required to maintain timely communication with the security organization when performing escort duties to summon assistance if needed. Vehicle escorts are required to maintain continuous communication with the security organization when performing escort duties to summon assistance if needed.

Section 73.55(h), Search Programs**.** This paragraph prescribes the search requirements of personnel, vehicles, and materials before granting access to the owner controlled and protected areas during normal and emergency conditions. The rule requires that a general description of the broad categories of material that will be excepted will be stated in the licensee security plans with detailed descriptions being identified in implementation procedures.

Section 73.55(i), Detection and Assessment Systems. This paragraph delineates the requirements for detection and assessment for operating reactors and applicants as applied to the physical protection program. Detection and assessment are addressed together as a consequence of their importance for ensuring that an adequate response can be initiated and completed as a result of an alarm or through surveillance observation and monitoring by security

personnel. Alarm stations are required to possess the equipment needed for detection, assessment, and communication or otherwise implement the protective strategy and maintain these capabilities through uninterruptible and secondary power sources. In addition, the survivability requirements for alarm stations pertaining to a single act within the capabilities of the design basis threat are addressed in this paragraph. The requirement to construct, locate, protect, and equip both the central and secondary alarm stations is applicable to only applicants for an operating or combined license that is issued after the effective date of this final rule. The rule requires that both alarms stations at future facilities will be equal and redundant.

Section 73.55(j), Communication Requirements. This paragraph stipulates the communication requirements for the security organization during normal and emergency conditions. The rule requires that the licensee security organization possesses and maintains the capability for continuous communication with internal security personnel, vehicle escorts, local law enforcement authorities, and the control room.

Section 73.55(k), Response Requirements. This paragraph outlines the provisions regarding the security response organization's structure, liaison with local law enforcement authorities, and measures to increase the security posture under heightened threat conditions. The rule requires that each licensee will determine the specific minimum number of armed responders and armed security officers needed to protect their facility and will document this minimum number in security plans. The threat warning system is intended to provide pre-planned enhancements to the licensee physical protection program to be taken upon notification by the NRC of a heightened threat. The specific details regarding response requirements are addressed in appendix C of this part.

Section 73.55(l), Facilities Using Mixed-Oxide (MOX) Fuel Assemblies Containing Up to 20 Weight Percent Plutonium Dioxide ($PuO_2$). This paragraph establishes the requirements for the physical protection of MOX used at nuclear power reactor facilities in addition to the physical

protection program requirements addressed by this section. These protective measures are necessary to account for the type of special nuclear material contained in MOX fuel assemblies. These additional requirements include measures for the search and inspection of MOX fuel assemblies, storage MOX fuel assemblies, material control and accounting, and controls for the use of fuel handling equipment used for the movement of MOX fuel assemblies.

Section 73.55(m), Security Program Reviews. This paragraph establishes requirements for the licensee's review of its physical protection programs. The rule requires that each licensee will review the physical protection program, in its entirety, at least every 24 months or less when significant changes are made. The conduct of reviews, to include audits is intended to provide a level of assurance that each element of the physical protection program is performing as intended to satisfy Commission requirements. Reviews also ensure that any changes to site specific conditions do not adversely impact the capability of a given element to perform the intended function within the physical protection program.

Section 73.55(n), Maintenance, Testing, and Calibration. This paragraph establishes requirements for the maintenance, testing, and calibration security equipment required to implement the physical protection program. The rule requires that each licensee will perform maintenance, testing, and calibration activities at intervals required to ensure the equipment is operating as intended. The conduct of maintenance, testing, and calibration activities is intended to provide a level of assurance that security equipment is performing within acceptable parameters established to support the physical protection program and satisfy Commission requirements. Specific intervals for maintenance, testing, and calibration are determined by the NRC and manufacturer specifications.

Section 73.55(o), Compensatory Measures. This paragraph establishes requirements for the actions to be taken by a licensee in response to a failure or degradation of security equipment to perform intended functions within the physical protection program. The rule

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

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

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

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

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

the license the ability to develop measures for the protection against radiological sabotage other than those specifically stated in Commission requirements. Licensee requests to employ such alternative measures must be submitted to the Commission for review and approval as a license amendment in accordance with § 50.90.

**K. Section 73.56, Personnel Access Authorization Requirements for Nuclear Power Plants.**

Section 73.56 (a), Introduction**.** This paragraph outlines the implementation, scope and applicability of the access authorization program and requires that this program be described in the licensee's physical security plan. Current licensees must be in compliance with the requirements described in this rule within 180 days of the rule's effective date including updating their site-specific security plans as applicable. Current licensees should update their plans using one of the processes described in 10 CFR 50.54(p), 10 CFR 50.90, or 10 CFR 73.5 as applicable. In addition, current applicants for an operating license or combined license as of the effective date of this rule must update their applications, as appropriate, to address the requirements of this section. Section 73.56 retains the intent of the pre-existing requirements that licensees have the authority to grant or deny an individual unescorted access, certify or deny an individual unescorted access authorization, or permit an individual to maintain or terminate unescorted access or unescorted access authorization. Additionally, the Commission allows applicants to certify or deny an individual unescorted access authorization status prior to receiving its operating license under part 50 of this chapter or before the Commission makes its finding under 10 CFR 52.103(g).

A licensee or applicant may allow a contractor or vendor to maintain certain elements of the licensee's or applicant's access authorization program if the contractor or vendor complies with the requirements of this section. Additionally, a licensee or applicant may permit a contractor or vendor to maintain an individual's unescorted access authorization status if the

contractor's or vendor's access authorization program includes the licensee's or applicant's approved behavioral observation program. However, licensees and applicants are responsible for meeting all of the requirements set forth in this section before granting an individual unescorted access or certifying an individual unescorted access authorization.

Applicants for an operating license or a combined license must incorporate their access authorization program in their physical security plan and implement the access authorization program before the receipt of special nuclear material in the form of fuel assemblies on site (i.e., within the licensee's protected area.)

Section 73.56(b), Individuals Subject to the Access Authorization Program. This paragraph identifies individuals who shall be subject to the requirements of an access authorization program to ensure that each person granted unescorted access and/or certified unescorted access authorization is trustworthy and reliable. The rule requires that any individual who has unescorted access to nuclear power plant protected and vital areas shall be subject to an access authorization program that meets the requirements of this section.

Section 73.56(c), General Performance Objective. This paragraph stipulates that the licensee's or applicant's access authorization program must provide high assurance that the individuals subject to this section are trustworthy and reliable such that they do not constitute an unreasonable risk to public health and safety or the common defense and security including the potential to commit radiological sabotage.

Section 73.56(d), Background Investigation. This paragraph outlines the responsibilities and elements of the background investigation process including consent; personal, employment, credit, and criminal history; identity verification; and character evaluation. As addressed with respect to § 73.56(h)(5) and (h)(6), the Commission permits licensees and applicants to meet the requirements of this section by relying on certain background investigation elements, psychological assessments, and behavioral observation training conducted by other licensees,

applicants, or contractor access programs.

This provision reduces regulatory burden by eliminating the need to replicate access authorization program elements that are still current according to the time conditions specified in §§ 73.56(h) and (i)(1).

Additionally, this paragraph requires individuals to disclose personal history information pertaining to the access authorization program and associated processes and requires licensees, applicants, and contractors or vendors to take steps to access information from reliable sources to ensure that the personal identifying information the individual has provided is authentic and accurate.

The rule requires licensees, applicants, and contractors or vendors to make available and disclose information that they have collected if contacted by another licensee, applicant, or contractor or vendor who has a release signed by the individual who is applying for unescorted access or unescorted access authorization.

Section 149 of the AEA provides the Commission authority to require individuals to be fingerprinted and to obtain the FBI criminal history records of only those individuals who are seeking unescorted access to protected or vital areas of a nuclear power plant. For other individuals, the Commission expects licensees and applicants to obtain those individual's criminal records in accordance with requirements set forth in § 73.56(k)(1)(ii).

Section 73.56(e), Psychological Assessment. This paragraph outlines requirements within the access authorization program for conducting psychological assessments on individuals seeking unescorted access or unescorted access authorization. The purpose of the paragraph is to evaluate the implications of an individual's psychological character on his or her trustworthiness and reliability. The rule requires that Individuals who are applying for initial unescorted access or unescorted access authorization, or who have not maintained unescorted access or unescorted access authorization for greater than 365 days, be subjected to a

psychological assessment.

This paragraph establishes requirements, standards, roles, and responsibilities for individuals who perform psychological assessments. A licensed psychologist or psychiatrist with proper clinical training and experience must conduct the psychological assessment in accordance with the American Psychological Association or the American Psychiatric Association standards. This paragraph establishes the responsibilities of those conducting psychological assessments to report the discovery of any information, including a medical condition, which could adversely impact the fitness for duty or trustworthiness and reliability of the individual being accessed.

Section 73.56(f), Behavioral Observation. This paragraph outlines the roles and responsibilities of licensees, applicants, contractors, vendors, and individuals under the behavioral observation program. The purpose of the behavioral observation program is to increase the likelihood that potentially adverse behavior patterns and actions are detected, communicated, and evaluated before there is an opportunity for such behavior patterns or acts to result in detrimental consequences. The rule requires individuals under this program to be trained to identify and report questionable behavior patterns or activities to his or her supervisor, other management personnel, or the reviewing official as designated in site procedures and that this report be promptly conveyed to the reviewing official for evaluation.

Section 73.56(g), Self-Reporting of Legal Actions. This paragraph outlines the responsibilities for individuals to self-report legal actions taken by a law enforcement authority or court of law to which the individual has been subject that could result in incarceration or a court order or that requires a court appearance. This paragraph requires the recipient of the report, if the recipient is not the reviewing official, to promptly convey the report to the reviewing official who will then evaluate the implications of those actions with respect to the individual's trustworthiness and reliability.

Section 73.56(h), Granting Unescorted Access and Certifying Unescorted Access Authorization. This paragraph defines the regulatory standard that must be used by a licensee or applicant for a determination of granting or certifying unescorted access or unescorted access authorization as well as for reinstatement of unescorted access or unescorted access authorization. The requirements in this paragraph, in part, are based upon whether an individual has previously been granted unescorted access or certified unescorted access authorization under a program subject to the requirements of § 73.56 and the elapsed time since the individual's unescorted access or unescorted access authorization status was last favorably terminated. Additionally, this paragraph provides requirements for re-establishing trustworthiness and reliability of those individuals whose unescorted access or unescorted access authorization was denied or terminated unfavorably. Sections 73.56(h)(5) and (6) permit licensees and applicants to rely on other access authorization programs that meet the requirements of this section. In addition, these provisions eliminate redundancies in the steps required for granting unescorted access or certifying unescorted access authorization or maintaining unescorted access or unescorted access authorization.

Section 73.56(i), Maintaining Unescorted Access or Unescorted Access Authorization. This paragraph delineates the conditions and requirements for maintaining unescorted access or unescorted access authorization status. Important elements of maintaining unescorted access or unescorted access authorization status are the behavioral observation program, the reevaluation of criminal history and credit history, and, for select individuals who perform specific job functions identified in § 73.56(i)(1)(B), a psychological assessment.

To confirm each individual's continued trustworthiness and reliability determination, the rule requires licensees and applicants to conduct updates and reevaluations every five (5) years for individuals granted unescorted access or certified unescorted access authorization and every three (3) years for selected individuals. For selected individuals, the rule requires licensees and

applicants to conduct psychological reassessments every five (5) years. Additionally, all individuals are required to be subject to the licensee's behavioral observation program on a daily basis to detect an individual's abnormal emotional and/or psychological state through monitoring and/or supervisory evaluation.

Section 73.56(j), Access to Vital Areas. This paragraph requires that access to vital areas be controlled through the use of access authorization lists to ensure that no one may enter these vital areas without having a work-related need and, when the need no longer exists, access to the vital areas is terminated.

The rule requires that access authorization lists will be updated at least every 31 days to minimize insider threats by ensuring that personnel listed have a continued need to access vital areas to perform their official duties and not just a possibility of needing access sometime in the future.

Section 73.56(k), Background Screeners. This paragraph outlines requirements to ensure that individuals who collect, process, or have access to sensitive personal information required under this section are trustworthy and reliable.

Background checks for these individuals must be conducted in accordance with the requirements of this paragraph. The Commission recognizes that licensees and applicants may not, under Section 149 of the AEA, obtain a fingerprint-based FBI criminal history records check for an individual who does not have or is not expected to have unescorted access. In such cases, local criminal history information about the individual will be obtained from the State or local court system to satisfy this requirement.

Section 73.56(l), Review Procedures. This paragraph outlines requirements for responding to an individual's request for review of a determination to deny unescorted access or unescorted access authorization or unfavorable termination of an individual's unescorted access or unescorted access authorization.

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

Section 73,56(n), Audits and Corrective Action. This paragraph outlines requirements for audits and corrective action to confirm compliance with the requirements of this section and that comprehensive corrective actions are taken in response to any violations of the requirements of this section identified from an audit. The rule requires that licensees and applicants will perform an audit of their access authorization program at intervals nominally every 24 months. With regard to § 73.56(n)(1), the Commission uses the term "nominally" which allows a 25 percent margin consistent with the definition of nominal in § 26.5, which provides limited flexibility in meeting the scheduled due date for completing this recurrent activity. Completing a recurrent activity at a nominal frequency means that the activity may be completed within a period that is 25 percent longer (30 months) or shorter (18 months) than the period required, with the next scheduled due date no later than the current scheduled due date plus the required frequency for completing the activity.

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

authorization program.

In regard to § 73.56(n)(7), the rule permits licensees and other entities to jointly conduct audits as well as to rely on one another's audits, if the audits upon which they are relying address the services obtained from the contractor or vendor by each of the sharing licensees or applicants. The rule requires that licensees, applicants, and contractors or vendors relying on a shared audit to ensure that all services and elements upon which they rely have been adequately audited and to make clear that the licensees, applicants, and contractors or vendors are responsible for ensuring that an adequate audit is conducted of any services or elements upon which they rely that are not adequately covered by the shared audit.

Section 73.56(o), Records**.** This paragraph outlines requirements for the retention, storage, and protection of records required by this section. Licensees, applicants, contractors, and vendors must retain, store, and protect records to ensure their availability and integrity. In addition, this paragraph provides requirements for how long the licensee shall retain these records according to the type of record or until the completion of legal proceedings that may arise as a result of an adjudication of an application for unescorted access, whichever is later. These requirements also allow contractors and vendors to retain records for which they are responsible. Upon termination of a contract between a contractor and a licensee or applicant, the licensee or applicant must retrieve all relevant records that were accumulated by the contractor throughout the period of the contract. The rule requires that corrected or new information will be actively communicated by the recipient to other licensees.

**L. Section 73.58, Safety/Security Interface Requirements for Nuclear Power Reactors.**

Section 73.58 is a new requirement added to part 73. This requirement makes explicit, what was previously implicitly required by the regulations including that plant activities should not adversely affect security activities and that security activities should not adversely affect plant

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

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

adverse effect. Managing the potential adverse effect is further described in paragraph (d). The requirements of § 73.58 are in addition to requirements to assess proposed changes and to manage potential adverse effects contained in other Commission regulations, and are not intended to substitute for them. The Commission recognizes that implementation of § 73.58 would rely to some extent on these existing programs that manage facility changes and configuration, and expects licensees to incorporate § 73.58 into this structure. The primary function of this rule is to explicitly require that licensees consider the potential for changes to cause adverse interaction between security and safety and to appropriately manage any adverse results. Documentation of assessments performed per paragraph (b) is not required so as not to delay plant or security actions unnecessarily.

Section 73.58(c) requires changes identified by either planned or emergent activities to be assessed by the licensee. This requirement is not intended to require licensees to assess all the day-to-day activities that are controlled by facility work processes and configuration management processes. The Commission expects that licensees would instead revise these processes to preclude, to the extent practicable, potential adverse interactions. Paragraph (c) of this section provides a description of typical activities for which changes must be assessed and for which resultant adverse interactions must be managed.

Section 73.58(d) requires that, when potential adverse interactions are identified, licensees communicate the potential adverse interactions to appropriate licensee personnel. The licensee is also required to take appropriate compensatory and mitigative actions to maintain safety and security consistent with the applicable Commission requirements. The compensatory and/or mitigative actions taken must be consistent with existing requirements for the affected activity.

**M. Part 73, Appendix B, General Criteria for Protection.**

The title of this appendix reflects training and qualification requirements for the members

of the security organization and other facility personnel who perform security related duties at a nuclear power reactor facility. The rule requires that individuals who perform security functions are trained and qualified prior to performing security-related duties and the training and qualification is documented.

Part 73, Appendix B, Section VI.A, General Requirements and Introduction. This paragraph highlights the minimum employment suitability and training and qualification program requirements for individuals selected to perform security related functions. All individuals who perform physical protection and/or contingency response duties within the security program must meet the minimum training and qualification requirements for their assigned duties as specified within this appendix and the Commission approved training and qualification plan. The word "individuals" is used to identify members of the security organization and those facility personnel who are assigned to perform physical protection or contingency response duties within the security program. Facility personnel performing physical protection duties need only meet the minimum training and qualification requirements specified within this appendix and the Commission approved training and qualification plan for the specific duty assigned. Where requirements under this appendix specifically apply to members of the security organization the language explicitly identifies this applicability.

Part 73, Appendix B, Section VI.B, Employment Suitability and Qualification. This paragraph outlines the minimum criteria that must be evaluated by licensees for individuals being considered for and performing security-related duties. The minimum criteria include education, criminal history, and physical and psychological standards.

The physical standards associated with this paragraph reflect the basic physical requirements that ensure an individual possesses the standard acuity levels associated with vision and hearing and that the individual does not have a medical condition that is detrimental to the individual's health or the performance of assigned duties. The standards posed are

applicable to all individuals who are assigned to perform physical protection or contingency response duties within the security program, to include non-security personnel assigned to perform physical protection duties (such as vehicle escort or material search). A licensed medical professional is required to conduct a medical examination before the assignment of individuals to perform security duties and/or the physical fitness test being administered.

The physical fitness test, which is required for armed individuals implementing the contingency response plan, is a performance-based test that must be designed to demonstrate an individual's physical ability to perform assigned security duties during contingency events. Before engaging in the physical fitness test, the individual's current health status must be verified by the licensee. The licensee is also required to confirm that there are no existing medical conditions which would be detrimental to the individual's health when placed under the physical stress induced by the physical fitness test. The licensed medical professional provides a certification of the individual's health before the test, but is not required to administer the physical fitness test or document or attest to the successful completion of the test. Scheduling the physical fitness test for each armed individual as soon as possible after the date of the physical examination required by paragraph B.2.a(2) minimizes the possibility of the individual incurring a medical condition from the time of examination to the time that the physical fitness test is administered.

The Commission recognized that the proposed suitability requirements for security personnel found in appendix B to part 73, criterion VI.B.1, were not inclusive of the disqualifying criteria found under the Gun Control Act of 1968 (GCA) (see 18 U.S.C. 922(g) and (n)). This section describes a licensee’s obligations to take those prohibitions into account prior to permitting an individual to serve as an armed security officer.

The rule requires that a qualified training instructor is responsible for the final documentation of each security critical task qualification that is performed by individuals who are

assigned physical protection and/or contingency response duties within the security program. This paragraph also enables members of the security organization who are medically disqualified from performing contingency response duties or specific physical protection duties for a period of time, to perform other physical protection duties that would not be affected by the medical disqualification.

Part 73, Appendix B, Section VI.C, Duty Training**.** This paragraph outlines duty training and on-the-job training requirements and focuses on the knowledge, skills, and abilities needed by individuals selected to perform security duties. On the job training for daily security duties may be conducted as a part of basic qualification training that provides the individual with the basic knowledge, skills and abilities of assigned securities duties. In addition to the on-the-job training previously described, this paragraph describes the development and implementation of 40 hours of on-the-job training to train the security force in the response to contingency events. It also captures both the scope of conducting tactical response drills and force-on-force exercises as well as the importance of individual performance by the members of the security response organization. The requirement is added to ensure that individuals implementing the safeguards contingency plan possess first-hand knowledge of individual and team response duties in accordance with the licensee protective strategy.

Part 73, Appendix B, Section VI.C.3, Performance Evaluation Program. This paragraph outlines the establishment of the performance evaluation program including individual and group requirements for security personnel participation. The Commission's intent is that the licensee's performance evaluation program be evaluated during the conduct of NRC security baseline inspections including force-on-force evaluations. The rule allows force-on-force exercises conducted to satisfy the NRC triennial evaluation requirement to be used to satisfy the annual force-on-force requirement for the personnel that participate in the capacity of the security response organization.

Part 73, Appendix B, Section VI.D, Duty Qualification and Re-qualification. This paragraph outlines the qualification, re-qualification, and periodicity requirements for armed and unarmed individuals performing security duties. The rule requires that qualifications include written exams, hands-on performance demonstrations, and annual written exams where applicable.

Part 73, Appendix B, Section VI.E, Weapons Training. This paragraph outlines the requirements for firearms training, firearms instructor qualifications, firearms familiarization training, training program elements, deadly force instruction, and weapons training periodicity. The Commission's intent is to make generically applicable requirements similar to those that were contained in the 2003 training and qualification order (EA-03-039) and experience gained through security program inspections and observations and to apply language consistent with the professional firearms community more accurately. Additionally, a list of common firearms practices are provided to ensure appropriate weapons training and qualification, safe handling, and operations are achieved.

Part 73, Appendix B, Section VI.F, Weapons Qualification and Requalification Program. This paragraph outlines the requirements for general and tactical weapons qualification, the types of qualification courses, courses of fire, and firearms requalification. These requirements are substantially similar to the weapons proficiency requirements that were stipulated in the 2002 training and qualification order and the commonly-accepted minimum qualification scores found in the firearms training community for shotguns, hand guns, semi-automatic and/or enhanced weapons during both day and night courses of fire.

Part 73, Appendix B, Section VI.G, Weapons, Personal Equipment, and Maintenance. This paragraph outlines the weapons, as well as required and optional personal equipment, for individuals performing security-related duties. The rule requires that the equipment required by paragraph G.2.b be readily accessible. The Commission does not intend that the required

equipment necessarily be carried or worn but intends that it be readily available should the security officer choose to wear it during a safeguards contingency event. The Commission's intent is that the optional equipment listed in paragraph G.2.c be considered for implementation consistent with the licensee's protective strategy. The paragraph also discusses the weapons maintenance program and certified armorer requirements. The armorer must be certified by the weapons manufacturer (or a contractor working on behalf of the manufacturer) to perform maintenance and repair of licensee firearms. Licensees may use a manufacturer's armorer and certification process or use a contractor certified by the manufacturer as an armorer to perform maintenance and repair of licensee firearms.

Part 73, Appendix B, Section VI.H, Records**.** This paragraph outlines the documentation and records retention requirements for security-related training. The Commission's intent is to be consistent with the record keeping and documentation requirements set forth in § 73.55(r).

Part 73, Appendix B, Section VI.I, Reviews. This paragraph outlines the required reviews of security-related training as set forth in § 73.55(n).

Part 73, Appendix B, Section VI.J, Definitions**.** This paragraph is consistent with the terms and definitions outlined in parts 50, 70, and 73.

**N. Part 73, Appendix C, Section II, Nuclear Power Plant Safeguards Contingency Plans.**

This section is revised to address nuclear power reactor safeguards contingency plan requirements without impacting other licensees who are also required to maintain safeguards contingency plans (SCP).

Part 73, Appendix C, Section II.A Introduction. This paragraph describes the content of the SCP for nuclear power reactors. Licensees must complete the coordination of the predetermined security force actions and non-security response efforts to ensure that the predetermined actions of the security force can be effectively implemented without conflict with

the actions of other onsite or offsite support agencies responding to a safeguards contingency event. The scope of the SCP is specific to the security organization. However, the safeguards contingency plan must be integrated with other onsite and offsite response plans and procedures. It is not the Commission's intent for the security organization to be responsible for the integrated response plan but rather to ensure coordination with the integrated response plan and other licensee organizational elements.

Part 73, Appendix C, Section II.B, Contents of the Plan**.** This paragraph specifies the categories of information required in a safeguards contingency plan to be consistent with and complement the requirements of § 50.34(d). The intent is to build a common approach to documenting SCP requirements and to improve the usefulness and applicability of the SCP, and to ensure that the SCP is coordinated with non-security response plans. The Commission does not intend that the SCP include the details of other site plans but rather intends to ensure that the licensee has considered these other plans and that potential conflicts have been identified and resolved.

Part 73, Appendix C, Section II.B.1, Background. This category of information requires licensees to identify perceived dangers, purpose, scope, and general information in the development and implementation of the SCP. The intent is to document the types of incidents that the plan covers, goals and objectives of the plan for each event, the physical protection elements that support the plan, and the coordination of response efforts by local law enforcement agencies. The NRC does not intend to expand the security organization's role or responsibilities to encompass the functions of other organizational elements. Planning functions and responsibilities of other licensee organizational elements are addressed in §§ 50.54(gg), 50.47, and part 50, appendix E.

Part 73, Appendix C, Section II.B.2, Generic Planning Base. This category of information establishes the criteria for initiating and terminating responses to safeguards contingency

events. The generic planning base must define specific decisions, actions, expectations, and supporting information needed to respond to each type of incident. This requirement focuses on the types of actions or information that will prompt the licensee to initiate and/or terminate response activities as a result of an actual or perceived threat to the facility.

Part 73, Appendix C, Section II.B.3, Licensee Planning Base. This category of information focuses on factors that affect safeguards contingency planning specific to each facility. The licensee planning base must document the site-specific organizational structure of the security response organization, site physical layout considerations, safeguards systems, the protective strategy, law enforcement assistance, policy constraints and assumptions and administrative and logistical considerations that could have bearing on the implementation of the licensee's SCP. While implementing details are appropriate for procedures and need not be included in the SCP, licensees are expected to provide a sufficient level of detail in the SCP for the information to be meaningful. Within this category of information, licensees must document coordination with off-site entities and explain how the level of protection required by § 73.55(b) during safeguards contingency events will be maintained. In addition, licensees must ensure that § 73.58 information regarding safety and security interface is considered in contingency response planning.

Part 73, Appendix C, Section II.B.4, Responsibility Matrix. This category of information documents responsibilities and specific actions to be taken by licensee organizations and/or personnel in response to safeguards contingency events. The responsibility matrix must document who will perform what actions and make what decisions during responses to safeguards contingency events. The licensee SCP's must discuss how the matrix is incorporated into site implementing procedures.

Part 73, Appendix C, Section II.B.5, Implementing Procedures. This category of information provides specific guidance and operating details that identify the actions to be taken

and decisions to be made by each member of the security organization who is assigned duties and responsibilities required for the effective implementation of the SCP. The procedures must reflect detailed information that supports the implementation of the SCP. The implementing procedures must contain the tabulated responsibility matrix that addresses each safeguards contingency event outlined in the licensee's generic planning base.

Part 73, Appendix C, Section II.C, Records and Reviews**.** This category of information requires licensees to maintain records and to conduct reviews in accordance with the requirements of § 73.55(n).

**V. Guidance.**

The Commission is preparing new regulatory guides that will contain detailed guidance on the implementation of the rule requirements. These regulatory guides, currently under development or already issued in draft form for comment will consolidate and update or eliminate previous guidance that was used to develop, review, and approve the power reactor security plans that licensees revised in response to the post-September 11, 2001, security orders. Development of the regulatory guides is ongoing and the publication of the final regulatory guides is planned shortly after the publication of this final rule. Some of these regulatory guides contain Safeguards Information (SGI) or Official Use Only – Security Related Information (OUO-SRI) and will only be available to those individuals with a need-to-know and who are qualified to have access to SGI or OUO-SRI as applicable. Where appropriate, the requirements in this final rule are adjusted to account for the lack of final guidance (e.g., if the guidance is needed to support a licensee or applicant submittal, then the submittal requirements are adjusted to account for the lack of final guidance).

**VI. Criminal Penalties.**

For the purposes of Section 223 of the Atomic Energy Act of 1954, as amended (AEA), the Commission is amending 10 CFR parts 50, 52, 72, and 73 under Sections 161b, 161i, or 161o of the AEA. Criminal penalties, as they apply to regulations in part 50, are discussed in § 50.111. Criminal penalties, as they apply to regulations in part 52, are discussed in § 52.303. Criminal penalties, as they apply to regulations in part 73, are discussed in § 73.81. The new §§ 50.54(hh), 73.54, and 73.58 are issued under Sections 161b, 161i, or 161o of the AEA, and are not included in §§ 50.111, 52.303, and 73.81(b) as applicable.

**VII. Availability of Documents.**

The NRC is making the documents identified below available to interested persons through one or more of the following methods:

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

*Regulations.gov (Web)*. These documents may be viewed and downloaded electronically through the Federal eRulemaking Portal http://www.Regulations.gov, Dockets NRC-2006-0016 and NRC-2008-0019.

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

| **Document** | **PDR** | **Web** | **ERR** (ADAMS) |
|---|---|---|---|
| Environmental Assessment | X | X | ML081640161 |
| Regulatory Analysis<br>Regulatory Analysis -appendices | X | X | ML081680069<br>ML081680090 |
| Information Collection Analysis | X | X | ML081780649 |
| Comment Response document | X | X | ML081690256 |

| | | | |
|---|---|---|---|
| EA-03-086, “Revised Design Basis Threat Order,” issued April 29, 2003 (68 FR 24517; May 7, 2003) [withheld as SGI and not publicly available.]* | X | X | ML030740002 |
| EA-02-026, “Interim Compensatory Measures (ICM) Order,” issued February 25, 2002 (67 FR 9792; March 4, 2002) [withheld as SGI and not publicly available.]* | X | X | ML020520754 |
| EA-02-261, “Issuance of Order for Compensatory Measures Related to Access Authorization,” issued January 7, 2003 (68 FR 1643; January 13, 2003) [withheld as SGI and not publicly available.]* | X | X | ML030060360 |
| EA-03-039, “Issuance of Order for Compensatory Measures Related to Training Enhancements on Tactical and Firearms Proficiency and Physical Fitness Applicable to Armed Nuclear Power Plant Security Force Personnel,” issued April 29, 2003 (68 FR 24514; May 7, 2003) [withheld as SGI and not publicly available.]* | X | X | ML030980015 |

*The NRC references these documents only for purposes of the backfitting discussion in this rule.

**VIII. 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 regulatory guidance currently under development. The NRC will consider using a voluntary consensus standard if an appropriate standard is

identified.

## IX. Finding of No Significant Environmental Impact.

The Commission has determined under the National Environmental Policy Act of 1969, as amended, and the Commission's regulations in Subpart A of 10 CFR part 51, that this rule is not 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 as a result of this action. The NRC requested comment on the environmental assessment. There were no comments received. Availability of the environmental assessment is provided in section VII of this document.

## X. Paperwork Reduction Act Statement.

This rule imposes new or amended information collection requirements contained in 10 CFR parts 50, 52, 72, and 73, that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501, *et seq*). These requirements were approved by the Office of Management and Budget, approval numbers 3150-0011, 3150-0151, 3150-0132, and 3150-0002.

The burden to the public for these information collections is estimated to average 4.38 hours per response. This includes the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments on any aspect of these information collections, including suggestions for reducing the burden, to the Records and FOIA/Privacy Services Branch (T-5-F53), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by Internet electronic mail to INFOCOLLECTS@NRC.GOV; and to the Desk Officer, Office of Information

and Regulatory Affairs, NEOB-10202, (3150-0011), Office of Management and Budget, Washington, DC 20503or by internet electronic mail to Nathan J. Frey@omb.eop.gov.

**XI. Regulatory Analysis.**

The Commission has prepared a regulatory analysis of this regulation. The analysis examines the costs and benefits of the alternatives considered by the Commission. Availability of the regulatory analysis is provided in Section VII of this document.

**XII. Regulatory Flexibility Certification.**

In accordance with the Regulatory Flexibility Act (5 U.S.C. 605(b)), the Commission certifies that this rule does not have a significant economic impact on a substantial number of small entities. This rule affects only the licensing and operation of nuclear power plants. The companies that own these plants 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).

**XIII. Backfit Analysis.**

With regard to the governing criteria in § 50.109, this rulemaking contains two different sets of requirements. The first set of requirements in this rulemaking are requirements similar to those that were previously imposed under one of the following orders issued after September 11, 2001:

- EA-02-026, “Interim Compensatory Measures (ICM) Order,”" issued February 25, 2002 (March 4, 2002; 67 FR 9792);
- EA-02-261, “Access Authorization Order,” issued January 7, 2003 (January 13, 2003; 68 FR 1643);

- EA-03-039, “Security Personnel Training and Qualification Requirements (Training) Order,”" issued April 29, 2003 (May 7, 2003; 68 FR 24514); and
- EA-03-086, “Revised Design Basis Threat Order,” issued April 29, 2003 (May 7, 2003; 68 FR 24517).

For this first set of requirements, the NRC has determined that they are not backfitting as defined by § 50.109(a)(1), and therefore, a backfit analysis is unnecessary for these requirements. Section 50.109(a)(1) defines backfitting as “the modification or addition to systems, structures, components or design of a facility … or the procedures or organization required to design, construct or operate a facility; any of which may result from a new or amended provision in the Commission rules….” This first set of requirements in the final rule contains numerous requirements substantially similar to those previously imposed by the orders identified above. In some cases, more specific detail may have been provided in this final rule for a particular requirement that corresponds with a requirement that had previously been in an order. The provisions in this first set impose requirements that are substantially similar to those previously imposed to current licensees under the orders and are consistent with the implementing guidance that has been issued to licensees subsequent to the orders. Therefore, the first set of requirements do not constitute backfits as defined by the rule because they would not result in a modification or addition to any systems, structures, components or design of an affected facility, or the procedures or organization required to design, construct, or operate an affected facility. In any event, the Commission has also determined that the requirements represented in this first set are those necessary to ensure that these facilities provide adequate protection to the health and safety of the public and are in accord with common defense and security. Therefore, no backfit analysis has been prepared with respect to these requirements.

The second set of requirements in this rulemaking are additions that do constitute backfits. The NRC evaluated the second set of requirements in the aggregate in accordance with

§ 50.109 to determine if the costs of implementing the rule would be justified by a substantial increase in public health and safety or common defense and security. The NRC finds that qualitative safety benefits of the provisions that qualify as backfits in this rulemaking, considered in the aggregate, would constitute a substantial increase in protection to public health and safety and the common defense and security and that the costs of this rule would be justified in view of the increase in protection to safety and security provided by the backfits embodied in the proposed rule. The backfit analysis is contained within section 4.2 of the regulatory analysis. Availability of the regulatory analysis is provided in section VII of this document.

**XIV. Congressional Review Act.**

Under the Congressional Review Act of 1996, the NRC has determined that this action is not a major rule and has verified this determination with the Office of Information and Regulatory Affairs of OMB.

**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 72**

Administrative practice and procedure, Criminal penalties, Manpower training programs, Nuclear materials, Occupational safety and health, Penalties, Radiation protection, Reporting and recordkeeping requirements, Security measures, Spent fuel, Whistleblowing.

**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 AEA, as amended; the Energy Reorganization Act of 1974, as amended; 5 U.S.C. 552 and 5 U.S.C. 553; the NRC is adopting the following amendments to 10 CFR parts 50, 52, 72, 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); sec. 651(e), Pub. L. 109-58, 119 Stat. 806-810 (42 U.S.C. 2014, 2021, 2021b, 2111).

Section 50.7 also issued under Pub. L. 95-601, sec. 10, 92 Stat. 2951 as amended by Pub. L. 102-486, sec. 2902, 106 Stat. 3123 (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 - 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, footnote 9 is removed and reserved, paragraphs (c), (d) and (e) are revised, and paragraph (i) is added to read as follows:

**§ 50.34 Contents of construction permit and operating license applications; technical information.**

* * * * *

(c) *Physical security plan*. (1) Each applicant for an operating license for a production or utilization facility that will be subject to §§ 73.50 and 73.60 of this chapter must include a physical security plan.

(2) Each applicant for an operating license for a utilization facility that will be subject to the requirements of § 73.55 of this chapter must include a physical security plan, a training and qualification plan in accordance with the criteria set forth in appendix B to part 73 of this chapter, and a cyber security plan in accordance with the criteria set forth in § 73.54 of this chapter.

(3) The physical security plan must describe how the applicant will meet the requirements of part 73 of this chapter (and part 11 of this chapter, if applicable, including the identification and description of jobs as required by § 11.11(a) of this chapter, at the proposed facility). Security plans must list tests, inspections, audits, and other means to be used to demonstrate compliance with the requirements of 10 CFR parts 11 and 73, if applicable.

(d) *Safeguards contingency plan.*

(1) Each application for a license to operate a production or utilization facility that will be subject to §§ 73.50 and 73.60 of this chapter must include a licensee safeguards contingency plan in accordance with the criteria set forth in section I of appendix C to part 73 of this chapter. The "implementation procedures" required per section I of appendix C to part 73 of this chapter do not have to be submitted to the Commission for approval.

(2) Each application for a license to operate a utilization facility that will be subject to § 73.55 of this chapter must include a licensee safeguards contingency plan in accordance with the criteria set forth in section II of appendix C to part 73 of this chapter. The "implementing procedures" required in section II of appendix C to part 73 of this chapter do not have to be submitted to the Commission for approval.

(e) *Protection against unauthorized disclosure*. Each applicant for an operating license for a production or utilization facility, who prepares a physical security plan, a safeguards contingency plan, a training and qualification plan, or a cyber security plan, shall protect the plans and other related Safeguards Information against unauthorized disclosure in accordance with the requirements of § 73.21 of this chapter.

* * * * *

(i) A description and plans for implementation of the guidance and strategies intended to maintain or restore core cooling, containment, and spent fuel pool cooling capabilities under the circumstances associated with the loss of large areas of the plant due to explosions or fire as required by § 50.54(hh)(2) of this chapter.

3. In § 50.54, paragraph (p)(1) is revised and paragraph (hh) is added to read as follows:

**§ 50.54 Conditions of licenses.**

* * * * *

(p)(1) The licensee shall prepare and maintain safeguards contingency plan procedures

in accordance with appendix C of part 73 of this chapter for affecting the actions and decisions contained in the Responsibility Matrix of the safeguards contingency plan. The licensee may not make a change which would decrease the effectiveness of a physical security plan, or guard training and qualification plan, or cyber security plan prepared under § 50.34(c) or § 52.79(a), or part 73 of this chapter, or of the first four categories of information (Background, Generic Planning Base, Licensee Planning Base, Responsibility Matrix) contained in a licensee safeguards contingency plan prepared under § 50.34(d) or § 52.79(a), or part 73 of this chapter, as applicable, without prior approval of the Commission. A licensee desiring to make such a change shall submit an application for amendment to the licensee's license under § 50.90.

* * * * *

(hh) (1) Each licensee shall develop, implement and maintain procedures that describe how the licensee will address the following areas if the licensee is notified of a potential aircraft threat:

(i) Verification of the authenticity of threat notifications;

(ii) Maintenance of continuous communication with threat notification sources;

(iii) Contacting all onsite personnel and applicable offsite response organizations;

(iv) Onsite actions necessary to enhance the capability of the facility to mitigate the consequences of an aircraft impact;

(v) Measures to reduce visual discrimination of the site relative to its surroundings or individual buildings within the protected area;

(vi) Dispersal of equipment and personnel, as well as rapid entry into site protected areas for essential onsite personnel and offsite responders who are necessary to mitigate the event; and

(vii) Recall of site personnel.

(2) Each licensee shall develop and implement guidance and strategies intended to

maintain or restore core cooling, containment, and spent fuel pool cooling capabilities under the circumstances associated with loss of large areas of the plant due to explosions or fire, to include strategies in the following areas:

(i) Fire fighting;

(ii) Operations to mitigate fuel damage; and

(iii) Actions to minimize radiological release.

(3) This section does not apply to a nuclear power plant for which the certifications required under § 50.82(a) or § 52.110(a)(1) of this chapter have been submitted.

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

4. 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 (42 U.S.C. 5841, 5842, 5846); sec. 1704, 112 Stat. 2750 (44 U.S.C. 3504 note).

5. In § 52.79, paragraphs (iii), (iv) are revised and redesignated as paragraphs (iv) and (v), and new paragraph (iii) is added as follows:

§ 52.79 Contents of applications; technical information in final safety analysis report.

(a) * * *

36 * * *

(iii) A cyber security plan in accordance with the criteria set forth in § 73.54 of this chapter;

(iv) A description of the implementation of the safeguards contingency plan, training and

qualification plan, and cyber security plan; and

(v) Each applicant who prepares a physical security plan, a safeguards contingency plan, a training and qualification plan, or a cyber security plan, shall protect the plans and other related Safeguards Information against unauthorized disclosure in accordance with the requirements of § 73.21 of this chapter.

* * * * *

6. In § 52.80, paragraph (d) is added to read as follows:

§ 52.80 Contents of applications; additional technical information.

* * * * *

(d) A description and plans for implementation of the guidance and strategies intended to maintain or restore core cooling, containment, and spent fuel pool cooling capabilities under the circumstances associated with the loss of large areas of the plant due to explosions or fire as required by § 50.54(hh)(2) of this chapter.

**PART 72--LICENSING REQUIREMENTS FOR THE INDEPENDENT STORAGE OF SPENT NUCLEAR FUEL, HIGH-LEVEL RADIOACTIVE WASTE, AND REACTOR-RELATED GREATER THAN CLASS C WASTE**

7. The authority citation for part 72 continues to read as follows:

**AUTHORITY:** Secs. 51, 53, 57, 62, 63, 65, 69, 81, 161, 182, 183, 184, 186, 187, 189, 68 Stat. 929, 930, 932, 933, 934, 935, 948, 953, 954, 955, as amended, sec. 234, 83 Stat. 444, as amended (42 U.S.C. 2071, 2073, 2077, 2092, 2093, 2095, 2099, 2111, 2201, 2232, 2233, 2234, 2236, 2237, 2238, 2282); sec. 274, Pub. L. 86-373, 73 Stat. 688, as amended (42 U.S.C. 2021); sec. 201, as amended, 202, 206, 88 Stat. 1242, as amended, 1244, 1246 (42 U.S.C. 5841, 5842, 5846); Pub. L. 95-601, sec. 10, 92 Stat. 2951 as amended by Pub. L. 102-486, sec. 7902, 106 Stat. 3123 (42 U.S.C. 5851); sec. 102, Pub. L. 91-190, 83 Stat. 853 (42 U.S.C. 4332); secs. 131,

132, 133, 135, 137, 141, Pub. L. 97-425, 96 Stat. 2229, 2230, 2232, 2241, sec. 148, Pub. L. 100-203, 101 Stat. 1330-235 (42 U.S.C. 10151, 10152, 10153, 10155, 10157, 10161, 10168); sec. 1704, 112 Stat. 2750 (44 U.S.C. 3504 note); sec. 651(e), Pub. L. 109–58, 119 Stat. 806-810 (42 U.S.C. 2014, 2021, 2021b, 2111).

Section 72.44(g) also issued under secs. 142(b) and 148(c), (d), Pub. L. 100-203, 101 Stat. 1330-232, 1330-236 (42 U.S.C. 10162(b), 10168(c), (d)). Section 72.46 also issued under sec. 189, 68 Stat. 955 (42 U.S.C. 2239); sec. 134, Pub. L. 97-425, 96 Stat. 2230 (42 U.S.C. 10154). Section 72.96(d) also issued under sec. 145(g), Pub. L. 100-203, 101 Stat. 1330-235 (42 U.S.C. 10165(g)). Subpart J also issued under secs. 2(2), 2(15), 2(19), 117(a), 141(h), Pub. L. 97-425, 96 Stat. 2202, 2203, 2204, 2222, 2224 (42 U.S.C. 10101, 10137(a), 10161(h)). Subparts K and L are also issued under sec. 133, 98 Stat. 2230 (42 U.S.C. 10153) and sec. 218(a), 96 Stat. 2252 (42 U.S.C. 10198).

8. In § 72.212, paragraphs (b)(5)(ii), (b)(5(iii), (b)(5)(iv), and (b)(5)(v) are revised to read as follows:

**§ 72.212 Conditions of general license issued under § 72.210.**

* * * * *

(b) * * *

(5) * * *

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

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

(iv) The observational capability required by § 73.55(i)(3) of this chapter as applied to a new protected area may be provided by a guard or watchman on patrol in lieu of closed circuit television.

(v) For the purpose of this general license, the licensee is exempt from requirements to interdict and neutralize threats in § 73.55 of this chapter.

* * * * *

PART 73 - PHYSICAL PROTECTION OF PLANTS AND MATERIALS

9. The authority citation for part 73 continues to read as follows:

**Authority:** Secs. 53, 161, 149, 68 Stat. 930, 948, as amended, sec. 147, 94 Stat. 780 (42 U.S.C. 2073, 2167, 2169, 2201): sec. 201, as amended, 204, 88 Stat. 1242, as amended, 1245, sec. 1701, 106 Stat. 2951, 2952, 2953 (42 U.SC. 5841, 5844, 2297f); sec.1704, 112 Stat. 2750 (44 U.S.C. 3504 note): Energy Policy Act of 2005, Pub. L. 109-58, 119 Stat. 594 (2005).

Section 73.1 also issued under sec. 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).

10. In § 73.8, paragraph (b) is revised and paragraph (c) is added 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, 73.20, 73.21, 73.24, 73.25, 73.26, 73.27, 73.37, 73.40, 73.45, 73.46, 73.50, 73.54,

73.55, 73.56, 73.57, 73.58, 73.60, 73.67, 73.70, 73.71, 73.72, 73.73, 73.74, and Appendices B, C, and G to this part.

(c) This part contains information collection requirements in addition to those approved under the control number specified in paragraph (a) of this section. The information collection requirement and the control numbers under which it is approved are as follows:

(1) in § 73.71, NRC Form 366i are approved under control number 3150-0104.

11. Section 73.54 is added to read as follows**:**

**§73.54 Protection of digital computer and communication systems and networks**

By **[Insert date 180 days after the effective date of the rule]** each licensee currently licensed to operate a nuclear power plant under part 50 of this chapter shall submit, as specified in § 50.4 and § 50.90 of this chapter, a cyber security plan that satisfies the requirements of this section for Commission review and approval. Each submittal must include a proposed implementation schedule. Implementation of the licensee's cyber security program must be consistent with the approved schedule. Current applicants for an operating license or combined license who have submitted their applications to the Commission prior to the effective date of this rule must amend their applications to include a cyber security plan consistent with this section.

(a) Each licensee subject to the requirements of this section shall provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in § 73.1.

(1) The licensee shall protect digital computer and communication systems and networks associated with:

(i) Safety-related and important-to-safety functions,

(ii) Security functions,

(iii) Emergency preparedness functions, including offsite communications; and

(iv) Support systems and equipment which, if compromised, would adversely impact safety, security or emergency preparedness functions.

(2) The licensee shall protect the systems and networks identified in paragraph (a)(1) of this section from cyber attacks that would:

(i) Adversely impact the integrity or confidentiality of data and/or software;

(ii) Deny access to systems, services, and/or data; and

(iii) Adversely impact the operation of systems, networks, and associated equipment.

(b) To accomplish this, the licensee shall:

(1) Analyze digital computer and communication systems and networks and identify those assets that must be protected against cyber attacks to satisfy paragraph (a) of this section,

(2) Establish, implement, and maintain a cyber security program for the protection of the assets identified in paragraph (b)(1) of this section, and;

(3) Incorporate the cyber security program as a component of the physical protection program.

(c) The cyber security program must be designed to:

(1) Implement security controls to protect the assets identified by paragraph (b)(1) of this section from cyber attacks;

(2) Apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to and recover from cyber attacks,

(3) Mitigate the adverse affects of cyber attacks, and;

(4) Ensure that the functions of protected assets identified by paragraph (b)(1) of this section are not adversely impacted due to cyber attacks.

(d) As part of the cyber security program, the licensee shall:

(1) Ensure that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training necessary to perform their assigned duties and responsibilities.

(2) Evaluate and manage cyber risks.

(3) Ensure that modifications to assets, identified by paragraph (b)(1) of this section, are evaluated before implementation to ensure that the cyber security performance objectives identified in (a)(1) are maintained.

(e) The licensee shall establish, implement, and maintain a cyber security plan that implements the cyber security program requirements of this section.

(1) The cyber security plan must describe how the requirements of this section will be implemented and must account for the site-specific conditions that affect implementation.

(2) The cyber security plan must include measures for incident response and recovery for cyber attacks. The cyber security plan must describe how the licensee will:

(i) Maintain the capability for timely detection and response to cyber attacks;

(ii) Mitigate the consequences of cyber attacks;

(iii) Correct exploited vulnerabilities; and

(iv) Restore affected systems, networks, and/or equipment affected by cyber attacks.

(f) The licensee shall develop and maintain written policies and implementing procedures to implement the cyber security plan. Policies, implementing procedures, site-specific analysis, and other supporting technical information used by the licensee need not be submitted for Commission review and approval as part of the cyber security plan but are subject to inspection by NRC staff on a periodic basis.

(g) The licensee shall review the cyber security program as a component of the physical security program in accordance with the requirements of § 73.55(m), including the periodicity requirements.

(h) The licensee shall retain all records and supporting technical documentation required to satisfy the requirements of this section 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.

12. 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 **[Insert date - 180 days - after the effective date of this final rule published in the *Federal Register*]**, each nuclear power reactor licensee, licensed under 10 CFR part 50, shall implement the requirements of this section through its Commission-approved Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, and Cyber Security Plan referred to collectively hereafter as "security plans." Current applicants for an operating license under 10 CFR part 50, or combined license under 10 CFR part 52 who have submitted their applications to the Commission prior to the effective date of this rule must amend their applications to include a cyber security plan consistent with this section.

(2) The security plans must identify, describe, and account for site-specific conditions that affect the licensee's capability to satisfy the requirements of this section.

(3) The licensee is responsible for maintaining the onsite physical protection program in accordance with Commission regulations through the implementation of security plans and written security implementing procedures.

(4) 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 implement the requirements of this section before fuel is allowed onsite (protected area).

(5) The Tennessee Valley Authority Watts Bar Nuclear Plant, Unit 2, holding a current construction permit under the provisions of part 50 of this chapter, shall meet the revised requirements in paragraphs (a) through (r) of this section as applicable to operating nuclear power reactor facilities.

(6) 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 that do not reference a standard design certification or reference a standard design certification issued after **[INSERT EFFECTIVE DATE OF FINAL RULE]** shall meet the requirement of § 73.55(i)(4)(iii).

(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) To satisfy the general performance objective of paragraph (b)(1) of this section, the physical protection program must protect against the design basis threat of radiological sabotage as stated in § 73.1.

(3) The physical protection program must be designed to prevent significant core damage and spent fuel sabotage. Specifically, the program must:

(i) Ensure that the capabilities to detect, assess, interdict, and neutralize threats up to and including the design basis threat of radiological sabotage as stated in § 73.1, are maintained at all times.

(ii) Provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure the

effectiveness of the physical protection program.

(4) The licensee shall analyze and identify site-specific conditions, including target sets, that may affect the specific measures needed to implement the requirements of this section and shall account for these conditions in the design of the physical protection program.

(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 security plans and licensee procedures.

(6) The licensee shall establish, maintain, and implement a performance evaluation program in accordance with appendix B to this part, to demonstrate and assess the effectiveness of armed responders and armed security officers to implement the licensee's protective strategy.

(7) The licensee shall establish, maintain, and implement an access authorization program in accordance with § 73.56 and shall describe the program in the Physical Security Plan.

(8) The licensee shall establish, maintain, and implement a cyber security program in accordance with § 73.54.

(9) The licensee shall establish, maintain, and implement an insider mitigation program and shall describe the program in the Physical Security Plan.

(i) The insider mitigation program must 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's capability to prevent significant core damage and spent fuel sabotage.

(ii) The insider mitigation program must contain elements from:

(A) The access authorization program described in § 73.56;

(B) The fitness-for-duty program described in part 26 of this chapter;

(C) The cyber security program described in § 73.54; and

(D) The physical protection program described in this section.

(10) The licensee shall use the site corrective action program to track, trend, correct and prevent recurrence of failures and deficiencies in the physical protection program.

(11) Implementation of security plans and associated procedures must be coordinated with other onsite plans and procedures to preclude conflict during both normal and emergency conditions.

(c) Security plans.

(1) Licensee security plans must describe:

(i) How the licensee will implement requirements of this section through the establishment and maintenance of a security organization, the use of security equipment and technology, the training and qualification of security personnel, the implementation of predetermined response plans and strategies, and the protection of digital computer and communication systems and networks.

(ii) Site-specific conditions that affect how the licensee implements Commission requirements.

(2) Protection of Security Plans. The licensee shall protect the security plans and other security-related information against unauthorized disclosure in accordance with the requirements of § 73.21.

(3) Physical Security Plan. The licensee shall establish, maintain, and implement a Physical Security Plan which describes how the performance objective and requirements set forth in this section will be implemented.

(4) Training and Qualification Plan. The licensee shall establish, maintain, and implement, and follow a Training and Qualification Plan that describes how the criteria set forth in appendix B, to this part, “General Criteria for Security Personnel,” will be implemented.

(5) Safeguards Contingency Plan. The licensee shall establish, maintain, and implement a Safeguards Contingency Plan that describes how the criteria set forth in appendix C, to this part, "Licensee Safeguards Contingency Plans," will be implemented.

(6) Cyber Security Plan. The licensee shall establish, maintain, and implement a Cyber Security Plan that describes how the criteria set forth in § 73.54 “Protection of Digital Computer and Communication systems and Networks” of this part will be implemented.

(7) Security implementing procedures.

(i) The licensee shall have a management system to provide for the development, implementation, revision, and oversight of security procedures that implement Commission requirements and the security plans.

(ii) Implementing procedures must document the structure of the security organization and detail the types of duties, responsibilities, actions, and decisions to be performed or made by each position of the security organization.

(iii) The licensee shall:

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

(B) Ensure that revisions to security implementing procedures satisfy the requirements of this section.

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

(d) <u>Security organization.</u>

(1) The licensee shall establish and maintain a security organization that is designed,

staffed, trained, qualified, and equipped to implement the physical protection program in accordance with the requirements of this section.

(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 security plans and the licensee protective strategy.

(3) The licensee may not permit any individual to implement any part of the physical protection program unless the individual has been trained, equipped, and qualified to perform their assigned duties and responsibilities in accordance with appendix B to this part and the Training and Qualification Plan. Non-security personnel may be assigned duties and responsibilities required to implement the physical protection program and shall:

(i) Be trained through established licensee training programs to ensure each individual is trained, qualified, and periodically re-qualified to perform assigned duties.

(ii) Be properly equipped to perform assigned duties.

(iii) Possess the knowledge, skills, and abilities, to include physical attributes such as sight and hearing, required to perform their assigned duties and responsibilities.

(e) Physical barriers. Each licensee shall identify and analyze site-specific conditions to determine the specific use, type, function, and placement of physical barriers needed to satisfy the physical protection program design requirements of § 73.55(b).

(1) The licensee shall:

(i) Design, construct, install and maintain physical barriers as necessary to control access into facility areas for which access must be controlled or denied to satisfy the physical

protection program design requirements of paragraph (b) of this section.

(ii) Describe in the security plan, physical barriers, barrier systems, and their functions within the physical protection program.

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

(3) Physical barriers must:

(i) Be designed and constructed to:

(A) Protect against the design basis threat of radiological sabotage;

(B) Account for site-specific conditions; and

(C) Perform their required function in support of the licensee physical protection program

(ii) Provide deterrence, delay, or support access control.

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

(4) Consistent with the stated function to be performed, openings in any barrier or barrier system established to meet the requirements of this section must be secured and monitored to prevent exploitation of the opening.

(5) Bullet Resisting Physical Barriers. 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.

(6) Owner controlled area. The licensee shall establish and maintain physical barriers in the owner controlled area as needed to satisfy the physical protection program design requirements of § 73.55(b).

(7) 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 observation and assessment of activities on either side of the protected area barrier;

(B) Monitored with intrusion detection equipment designed to satisfy the requirements of § 73.55(i) and be capable of detecting both attempted and actual penetration of the protected area perimeter barrier before completed penetration of the protected area perimeter barrier; and

(C) Monitored with assessment equipment designed to satisfy the requirements of §73.55(i) and provide real-time and play-back/recorded video images of the detected activities before and after each alarm annunciation.

(ii) Obstructions that could prevent the licensee's capability to meet the observation and assessment requirements of this section must be located outside of the isolation zone.

(8) Protected area.

(i) The protected area perimeter must be protected by physical barriers that are designed and constructed to:

(A) Limit access into the protected area to only those personnel, vehicles, and materials required to perform official duties;

(B) Channel personnel, vehicles, and materials to designated access control portals; and

(C) Be separated from any other barrier designated as a vital area physical barrier, unless otherwise identified in the Physical Security Plan.

(ii) Penetrations through the protected area barrier must be secured and monitored in a manner that prevents or delays, and detects the exploitation of any penetration.

(iii) All emergency exits in the protected area must be alarmed and secured by locking devices that allow prompt egress during an emergency and satisfy the requirements of this section for access control into the protected area.

(iv) Where building walls or roofs comprise a portion of the protected area perimeter

barrier, an isolation zone is not necessary provided that the detection and, assessment requirements of this section are met, appropriate barriers are installed, and the area is described in the security plans.

(v) All exterior areas within the protected area, except for areas that must be excluded for safety reasons, must be periodically checked to detect and deter unauthorized personnel, vehicles, and materials.

(9) Vital areas.

(i) Vital equipment must be located only within vital areas, which must be located within a protected area so that access to vital equipment requires passage through at least two physical barriers, except as otherwise approved by the Commission and identified in the security plans.

(ii) The licensee shall protect all vital area access portals and vital area emergency exits with intrusion detection equipment and locking devices that allow rapid egress during an emergency and satisfy the vital area entry control requirements of this section.

(iii) Unoccupied vital areas must be locked and alarmed.

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

(v) At a minimum, the following shall be considered vital areas:

(A) The reactor control room;

(B) The spent fuel pool;

(C) The central alarm station; and

(D) The secondary alarm station in accordance with § 73.55(i)(4)(iii).

(vi) At a minimum, the following shall be located within a vital area:

(A) The secondary power supply systems for alarm annunciation equipment; and

(B) The secondary power supply systems for non-portable communications equipment.

(10) Vehicle control measures. Consistent with the physical protection program design

requirements of § 73.55(b), the licensee shall protect against vehicle use as a means of transporting unauthorized personnel or materials to gain proximity to a protected area or vital area, or otherwise penetrate the protected area perimeter.

(i) Land vehicles. Licensees shall:

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

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

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

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

(11) Waterways. The licensee shall:

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

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

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

(f) Target sets.

(1) The licensee shall document and maintain the process used to develop and identify target sets, to include the site-specific analyses and methodologies used to determine and group the target set equipment or elements.

(2) The licensee shall consider cyber attacks in the development and identification of target sets.

(3) Target set equipment or elements that are not contained within a protected or vital area must be identified and documented consistent with the requirements in § 73.55(f)(1) and be accounted for in the licensee's protective strategy.

(4) The licensee shall implement a process for the oversight of target set equipment and systems to ensure that changes to the configuration of the identified equipment and systems are considered in the licensee's protective strategy. Where appropriate, changes must be made to documented target sets.

(g) Access controls.

(1) Consistent with the function of each barrier or barrier system, the licensee shall control personnel, vehicle, and material access, as applicable, at each access control point in accordance with the physical protection program design requirements of § 73.55(b).

(i) To accomplish this, the licensee shall:

(A) Locate access control portals outside of, or concurrent with, the physical barrier system through which it controls access.

(B) Equip access control portals with locking devices, intrusion detection equipment, and surveillance equipment consistent with the intended function.

(C) Provide supervision and control over the badging process to prevent unauthorized

bypass of access control equipment located at or outside of the protected area.

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

(E) The licensee shall assign an individual the responsibility for the last access control function (controlling admission to the protected area) and shall isolate the individual within a bullet-resisting structure to assure the ability of the individual to respond or summon assistance.

(ii) Where vehicle barriers are established, the licensee shall:

(A) Physically control vehicle barrier portals to ensure only authorized vehicles are granted access through the barrier.

(B) Search vehicles and materials for contraband or other items which could be used to commit radiological sabotage in accordance with paragraph (h) of this section.

(C) Observe search functions to ensure a response can be initiated if needed.

(2) Before granting access into the protected area, the licensee shall:

(i) Confirm the identity of individuals.

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

(iii) Confirm, in accordance with industry shared lists and databases that individuals are not currently denied access to another licensed facility.

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

(3) Vehicles in the protected area.

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

(ii) Vehicles inside the protected area must be operated by an individual authorized unescorted access to the area, or must be escorted by an individual as required by paragraph

(g)(8) of this section.

(iii) Vehicle use inside the protected area must be limited to plant functions or emergencies, and keys must be removed or the vehicle otherwise 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.

(4) Vital Areas.

(i) Licensees shall control access into vital areas consistent with access authorization lists.

(ii) In response to a site-specific credible threat or other credible information, implement a two-person (line-of-sight) rule for all personnel in vital areas so that no one individual is permitted access to a vital area.

(5) 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) To satisfy the design criteria of paragraph (g)(5)(i) of this section during emergency conditions, the licensee shall implement security procedures to ensure that authorized emergency personnel are provided prompt access to affected areas and equipment.

(6) Access control devices.

(i) The licensee shall control all keys, locks, combinations, passwords and related access control devices used to control access to protected areas, vital areas and security systems to reduce the probability of compromise. To accomplish this, the licensee shall:

(A) Issue access control devices only to individuals who have unescorted access authorization and require 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 or when a person with access to control devices has been terminated under less than favorable conditions.

(ii) The licensee shall implement a numbered photo identification badge 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 badges have been issued.

(iii) Access authorization program personnel shall be issued passwords and combinations to perform their assigned duties and may be excepted from the requirement of paragraph (g)(6)(i)(A) of this section provided they meet the background requirements of § 73.56.

(7) Visitors.

(i) The licensee may permit escorted access to protected and vital areas to individuals who have not been granted unescorted access 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 an escort is required.

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

(F) Deny escorted access to any individual who is currently denied access in industry shared data bases.

(ii) Individuals not employed by the licensee but who require frequent or extended unescorted access to the protected area and/or vital areas to perform duties and responsibilities required by the licensee at irregular or intermittent intervals, 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 and vital areas. Non-employee photo identification badges must visually reflect that the individual is a non-employee and that no escort is required.

(8) Escorts. The licensee shall ensure that all escorts are trained to perform escort duties in accordance with the requirements of this section and site training requirements.

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

(ii) Individuals assigned to visitor escort duties shall be provided a means of timely

communication with security personnel to summon assistance when needed.

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

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

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

(h) Search programs.

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

(2) Owner controlled area searches.

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

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

(iii) Vehicle searches must be performed by at least two (2) trained and equipped security personnel, one of which must be armed. The armed individual shall be positioned to observe the search process and provide immediate response.

(iv) Vehicle searches must be accomplished through the use of equipment capable of detecting firearms, explosives, incendiary devices, or other items which could be used to commit radiological sabotage, or through visual and physical searches, or both, to ensure that all items are identified before granting access.

(v) Vehicle access control points must be equipped with video surveillance equipment that is monitored by an individual capable of initiating a response.

(3) Protected area searches. Licensees shall search all personnel, vehicles and materials requesting access to protected areas.

(i) The search for firearms, explosives, incendiary devices, or other items which could be used to commit radiological sabotage shall be accomplished through the use of equipment capable of detecting these items, or through visual and physical searches, or both, to ensure that all items are clearly identified before granting access to protected areas. The licensee shall subject all persons except official Federal, state, and local law enforcement personnel on official duty to these searches upon entry to the protected area. Armed security officers who are on duty and have exited the protected area may re-enter the protected area without being searched for firearms.

(ii) Whenever search equipment is out of service, is not operating satisfactorily, or cannot be used effectively to search individuals, vehicles, or materials, a visual and physical search shall be conducted.

(iii) When an attempt to introduce firearms, explosives, incendiary devices, or other items which could be used to commit radiological sabotage has occurred or is suspected, the licensee shall implement actions to ensure that the suspect individuals, vehicles, and materials

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

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

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

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

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

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

(i) Detection and assessment systems.

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

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

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

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

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

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

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

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

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

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

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

(4) Alarm stations.

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

(A) Detect and assess alarms.

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

(C) Summon offsite assistance.

(D) Provide command and control.

(ii) Licensees shall:

(A) Locate the central alarm station inside a protected area. The interior of the central alarm station must not be visible from the perimeter of the protected area.

(B) Continuously staff each alarm station with at least one trained and qualified alarm station operator. The alarm station operator must not be assigned other duties or responsibilities which would interfere with the ability to execute the functions described in § 73.55(i)(4)(i) of this section.

(C) Not permit any activities to be performed within either alarm station that would interfere with an alarm station operator's ability to execute assigned duties and responsibilities.

(D) Assess and initiate response to all alarms in accordance with the security plans and implementing procedures.

(E) Assess and initiate response to other events as appropriate.

(F) Ensure that an alarm station operator cannot change the status of a detection point or deactivate a locking or access control device at a protected or vital area portal, without the knowledge and concurrence of the alarm station operator in the other alarm station.

(G) Ensure that operators in both alarm stations are knowledgeable of final disposition of all alarms.

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

(iii) 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 construct, locate, protect, and equip both the central and secondary alarm stations to the standards for the central alarm station contained in this section. Both alarm stations shall be equal and redundant, such that all functions needed to satisfy the requirements of this section can be performed in both alarm stations.

(5) Surveillance, observation, and monitoring.

(i) The physical protection program must include surveillance, observation, and monitoring as needed to satisfy the design requirements of §73.55(b), identify indications of tampering, or otherwise implement the site protective strategy.

(ii) The licensee shall provide continuous surveillance, observation, and monitoring of the owner controlled area as described in the security plans to detect and deter intruders and ensure the integrity of physical barriers or other components and functions of the onsite physical protection program. Continuous surveillance, observation, and monitoring responsibilities may be performed by security personnel during continuous patrols, through use of video technology, or by a combination of both.

(iii) Unattended openings that intersect a security boundary such as underground pathways must be protected by a physical barrier and monitored by intrusion detection equipment or observed by security personnel at a frequency sufficient to detect exploitation.

(iv) Armed security patrols shall periodically check external areas of the protected area to include physical barriers and vital area portals.

(v) Armed security patrols shall periodically inspect vital areas to include the physical barriers used at all vital area portals.

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

(vii) Security personnel shall be trained to recognize obvious indications of tampering consistent with their assigned duties and responsibilities.

(viii) Upon detection of tampering, or other threats, the licensee shall initiate response in accordance with the security plans and implementing procedures.

(6) Illumination.

(i) The licensee shall ensure that all areas of the facility are provided with illumination

necessary to satisfy the design requirements of § 73.55(b) and implement the protective strategy.

(ii) The licensee shall provide a minimum illumination level of 0.2 foot-candles, measured horizontally at ground level, in the isolation zones and appropriate exterior areas within the protected area. Alternatively, the licensee may augment the facility illumination system by means of low-light technology to meet the requirements of this section or otherwise implement the protective strategy.

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

(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 security plans and the licensee's procedures.

(3) All on-duty security force personnel shall be capable of maintaining continuous communication with an individual in each alarm station, and vehicles escorts shall maintain continuous communication with security personnel. All personnel escorts shall maintain timely communication with the security personnel.

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

(i) Radio or microwave transmitted two-way voice communication, either directly or through an intermediary, in addition to conventional telephone service between local law enforcement authorities and the site.

(ii) A system for communication with the control room.

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

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

(k) Response requirements.

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

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

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

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

(5) Armed responders.

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

licensee shall document this number in the security plans.

(ii) The number of armed responders shall not be less than ten (10).

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

(6) Armed security officers.

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

(ii) The minimum number of armed security officers designated to strengthen onsite response capabilities must be documented in the security plans.

(7) The licensee shall have procedures to reconstitute the documented number of available armed response personnel required to implement the protect strategy.

(8) Protective strategy. The licensee shall establish, maintain, and implement a written protective strategy in accordance with the requirements of this section and part 73, appendix C, Section II. Upon receipt of an alarm or other indication of a threat, the licensee shall:

(i) Determine the existence and level of a threat in accordance with pre-established assessment methodologies and procedures.

(ii) Initiate response actions to interdict and neutralize the threat in accordance with the requirements of part 73, appendix C, section II, the safeguards contingency plan, and the licensee's response strategy.

(iii) Notify law enforcement agencies (local, State, and Federal law enforcement agencies (LLEA)), in accordance with site procedures.

(9) Law enforcement liaison. To the extent practicable, licensees shall document and maintain current agreements with applicable law enforcement agencies to include estimated response times and capabilities.

(10) Heightened security. Licensees shall establish, maintain, and implement a threat warning system which identifies specific graduated protective measures and actions to be taken to increase licensee preparedness against a heightened security threat.

(i) Licensees shall ensure that the specific protective measures and actions identified for each threat level are consistent with the security plans and other emergency plans and procedures.

(ii) Upon notification by an authorized representative of the Commission, licensees shall implement the specific threat level indicated by the Commission representative.

(l) Facilities using mixed-oxide (MOX) fuel assemblies containing up to 20 weight percent plutonium dioxide ($PuO_2$).

(1) Commercial nuclear power reactors licensed under 10 CFR parts 50 or 52 and authorized to use special nuclear material in the form of MOX fuel assemblies containing up to 20 weight percent $PuO_2$ shall, in addition to meeting the requirements of this section, protect un-irradiated MOX fuel assemblies against theft or diversion as described in this paragraph.

(2) Commercial nuclear power reactors authorized to used MOX fuel assemblies containing up to 20 weight percent $PuO_2$ are exempt from the requirements of §§ 73.20, 73.45, and 73.46 for the onsite physical protection of un-irradiated MOX fuel assemblies.

(3) Administrative controls.

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

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

(iii) Upon receipt of un-irradiated MOX fuel assemblies, the licensee shall:

(A) Inspect un-irradiated MOX fuel assemblies for damage.

(B) Search un-irradiated 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 un-irradiated MOX fuel assemblies as follows:

(A) At least one armed security officer shall be present during the receipt and inspection of un-irradiated MOX fuel assemblies. This armed security officer shall not be an armed responder as required by paragraph (k) of this section.

(B) The licensee shall store un-irradiated MOX fuel assemblies only within a spent fuel pool, located within a vital area, so that access to the un-irradiated MOX fuel assemblies requires passage through at least two physical barriers and the water barrier combined with the additional measures detailed in this section.

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

(4) Physical controls.

(i) The licensee shall lock, lockout, or disable all equipment and power supplies to equipment required for the movement and handling of un-irradiated MOX fuel assemblies when movement activities are not authorized.

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

(iii) The licensee shall conduct random patrols of areas containing un-irradiated MOX fuel assemblies to identify indications of tampering and ensure the integrity of barriers and locks.

(iv) Locks, keys, and any other access control device used to secure equipment and

power sources required for the movement of un-irradiated MOX fuel assemblies, or openings to areas containing un-irradiated 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 un-irradiated MOX fuel assemblies or openings to areas containing un-irradiated 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 un-irradiated MOX fuel assemblies before the removal of the locks and providing power to equipment required for the movement or handling of un-irradiated 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 knowledgeable of authorized and unauthorized activities involving un-irradiated MOX fuel assemblies.

(5) At least one armed security officer shall be present and shall maintain constant surveillance of un-irradiated 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, interdict and neutralize threats to un-irradiated MOX fuel assemblies in accordance with the requirements of this section.

(7) MOX fuel assemblies containing greater than 20 weight percent $PuO_2$.

(i) Requests for the use of MOX fuel assemblies containing greater than 20 weight percent $PuO_2$ shall be reviewed and approved by the Commission before receipt of MOX fuel assemblies.

(ii) Additional measures for the physical protection of un-irradiated MOX fuel assemblies containing greater than 20 weight percent $PuO_2$ shall be determined by the Commission on a case-by-case basis and documented through license amendment in accordance with 10 CFR 50.90.

(m) Security program reviews.

(1) As a minimum the licensee shall review each element of the physical protection program at least every 24 months. Reviews shall be conducted:

(i) Within 12 months following initial implementation of the physical protection program or a change to personnel, procedures, equipment, or facilities that potentially could adversely affect security.

(ii) As necessary based upon site-specific analyses, assessments, or other performance indicators.

(iii) By individuals independent of those personnel responsible for program management and any individual who has direct responsibility for implementing the onsite physical protection program.

(2) Reviews of the security program must include, but not be limited to, an audit of the effectiveness of the physical security program, security plans, implementing procedures, cyber security programs, safety/security interface, activities, testing, maintenance, and calibration program, and response commitments by local, State, and Federal law enforcement authorities.

(3) The results and recommendations of the onsite physical protection program reviews, 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. These reports must be maintained in an auditable form, available for inspection.

(4) Findings from onsite physical protection program reviews must be entered into the site corrective action program.

(n) Maintenance, testing, and calibration.

(1) The licensee shall:

(i) Establish, maintain, and implement a maintenance, testing and calibration program to ensure that security systems and equipment, including secondary and uninterruptible power supplies, are tested for operability and performance at predetermined intervals, maintained in operable condition, and are capable of performing their intended functions.

(ii) Describe the maintenance, testing and calibration program in the 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, and the intervals or frequency at which the activity will be performed.

(iii) Identify in procedures the criteria for determining when problems, failures, deficiencies, and other findings are documented in the site corrective action program for resolution.

(iv) Ensure that information documented in the site corrective action program is written in a manner that does not constitute safeguards information as defined in 10 CFR 73.21

(v) Implement compensatory measures that ensure the effectiveness of the onsite physical protection program when there is a failure or degraded operation of security-related component or equipment.

(2) The licensee shall test each intrusion alarm 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 security plans and implementing procedures.

(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 local law enforcement agencies, to include backup 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.

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

(8) Security equipment or systems shall be tested in accordance with the site maintenance, testing and calibration procedures before being placed back in service after each repair or inoperable state.

(o) Compensatory measures.

(1) The licensee shall identify criteria and measures to compensate for degraded or inoperable equipment, systems, and components to meet the requirements of this section.

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

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

(p) Suspension of security 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 security measures under 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 security measures must be approved as a minimum by a licensed senior operator before taking this action.

(ii) During severe weather when the suspension of affected security measures is immediately needed to protect the personal health and safety of security force personnel and no other immediately apparent action consistent with the license conditions and technical specifications can provide adequate or equivalent protection. This suspension of security measures must be approved, as a minimum, by a licensed senior operator, with input from the security supervisor or manager, before taking this action.

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

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

(q) Records.

(1) The Commission may inspect, copy, retain, and remove all reports, records, and documents required to be kept by Commission regulations, orders, or license conditions, whether the reports, records, and documents 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, 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.

(3) 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.

(4) Review and audit reports must be maintained and available for inspection, for a period of three (3) years.

(r) 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 objectives and requirements specified in paragraph (b) of this section; and

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

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

(3) In addition to fully describing the desired changes, the licensee shall submit a technical basis for each proposed alternative measure. The basis must include an analysis or assessment that demonstrates how 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 vehicle barrier systems required by § 73.55(e)(10), the licensee shall demonstrate that:

(i) The alternative measure provides protection against the use of a vehicle as a means of transportation to gain proximity to vital areas;

(ii) The alternative measure provides protection against the use of a vehicle as a vehicle bomb; and

(iii) 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.

13. Section 73.56 is revised to read as follow:

**§ 73.56 Personnel access authorization requirements for nuclear power plants.**

(a) Introduction.

(1) By **[Insert date—180 days—after the effective date of the final rule published in the Federal Register]**, each nuclear power reactor licensee, licensed under 10 CFR part 50, shall implement the requirements of this section through revisions to its Commission-approved Physical Security Plan.

(2) The licensee shall establish, implement and maintain its access authorization program in accordance with the requirements of this section.

(3) Each applicant for an operating license under the provisions of part 50 of this chapter, and each holder of a combined license under the provisions of part 52 of this chapter, shall implement the requirements of this section before fuel is allowed on site (protected area).

(4) The licensee or applicant may accept, in part or whole, an access authorization program implemented by a contractor or vendor to satisfy appropriate elements of the licensee's access authorization program in accordance with the requirements of this section. Only a licensee shall grant an individual unescorted access. Licensees and applicants shall certify individuals' unescorted access authorization and are responsible to maintain, deny, terminate, or

withdraw unescorted access authorization.

(b) Applicability

(1) The following individuals shall be subject to an access authorization program:

(i) Any individual to whom a licensee intends to grant unescorted access to nuclear power plant protected or vital areas or any individual for whom a licensee or an applicant intends to certify unescorted access authorization;

(ii) Any individual whose duties and responsibilities permit the individual to take actions by electronic means, either on site or remotely, that could adversely impact the licensee's or applicant's operational safety, security, or emergency preparedness;

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

(iv) The licensee or applicant access authorization program reviewing official or contractor or vendor access authorization program reviewers.

(2) Other individuals, at the licensee's or applicant's discretion, including employees of a contractor or a vendor who are designated in access authorization program procedures, are subject to an access authorization program that meets the requirements of this section.

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

(d) Background investigation. In order to grant an individual unescorted access to the protected area or vital area of a nuclear power plant or certify an individual unescorted access authorization, licensees, applicants and contractors or vendors shall ensure that the individual

has been subject to a background investigation. The background investigation must include, but is not limited to, the following elements:

(1) Informed consent. Licensees, applicants, and contractors or vendors shall not initiate any element of a background investigation without the informed and signed consent of the subject individual. This consent shall include authorization to share personal information with appropriate entities. The licensee or applicant to whom the individual is applying for unescorted access and unescorted access authorization, respectively, or the contractors or vendors supporting the licensee or applicant shall inform the individual of his or her right to review information collected to assure its accuracy, and provide the individual with an opportunity to correct any inaccurate or incomplete information that is developed by licensees, applicants, or contractors or vendors about the individual.

(i) The subject individual may withdraw his or her consent at any time. Licensees, applicants, and contractors or vendors shall inform the individual that:

(A) Withdrawal of his or her consent will remove the individual's application for access authorization under the licensee's or applicant's access authorization program or contractor or vendor access authorization program; and

(B) Other licensees and applicants shall have access to information documenting the withdrawal. Additionally, the contractors or vendors may have the same access to the information, if such information is necessary for assisting licensees or applicants complying with requirements set forth in this section.

(ii) If an individual withdraws his or her consent, licensees, applicants, and contractors or vendors may not initiate any elements of the background investigation that were not in progress at the time the individual withdrew his or her consent, but shall complete any background investigation elements that are in progress at the time consent is withdrawn. The licensee or applicant shall record the status of the individual's application for unescorted access or

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

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

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

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

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

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

(2) Personal history disclosure.

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

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

disclose an administrative withdrawal of unescorted access or unescorted access authorization under the requirements of § 73.56(g), (h)(7), or (i)(1)(v) of this section. However, the individual must disclose this information if the individual's unescorted access or unescorted access authorization is administratively withdrawn at the time he or she is seeking unescorted access or unescorted access authorization, or the individual's unescorted access or unescorted access authorization was subsequently denied or terminated unfavorably by a licensee, applicant, or contractor or vendor.

(3) Verification of true identity. Licensees, applicants, and contractors or vendors shall verify the true identity of an individual who is applying for unescorted access or unescorted access authorization in order to ensure that the applicant is the person that he or she has claimed to be. At a minimum, licensees, applicants, and contractors or vendors shall validate that the social security number that the individual has provided is his or hers, and, in the case of foreign nationals, validate the claimed non-immigration status that the individual has provided is correct. In addition, licensees and applicants shall also determine whether the results of the fingerprinting required under § 73.57 confirm the individual's claimed identity, if such results are available.

(4) Employment history evaluation. Licensees, applicants, and contractors or vendors shall ensure that an employment history evaluation has been completed on a best effort basis, by questioning the individual's present and former employers, and by determining the activities of the individual while unemployed.

(i) For the claimed employment period, the individual must provide the reason for any termination, eligibility for rehire, and other information that could reflect on the individual's trustworthiness and reliability.

(ii) If the claimed employment was military service the individual shall provide a characterization of service, reason for separation, and any disciplinary actions that could affect a

trustworthiness and reliability determination.

(iii) If education is claimed in lieu of employment, the individual shall provide any information related to the claimed education that could reflect on the individual's trustworthiness and reliability and, at a minimum, verify that the individual was registered for the classes and received grades that indicate that the individual participated in the educational process during the claimed period.

(iv) If a previous employer, educational institution, or any other entity with which the individual claims to have been engaged fails to provide information or indicates an inability or unwillingness to provide information within 3 business days of the request, the licensee, applicant, or contractor or vendor shall:

(A) Document this refusal or unwillingness in the licensee's, applicant's, or contractor's or vendor's record of the investigation; and

(B) Obtain a confirmation of employment, educational enrollment and attendance, or other form of engagement claimed by the individual from at least one alternate source that has not been previously used.

(v) When any licensee, applicant, contractor, or vendor is seeking the information required for an unescorted access or unescorted access authorization decision under this section and has obtained a signed release from the subject individual authorizing the disclosure of such information, other licensees, applicants, contractors and vendors shall make available the personal or access authorization information requested regarding the denial or unfavorable termination of unescorted access or unescorted access authorization.

(vi) In conducting an employment history evaluation, the licensee, applicant, contractor, or vendor may obtain information and documents by electronic means, including, but not limited to, telephone, facsimile, or email. Licensees, applicants, contractors, or vendors shall make a record of the contents of the telephone call and shall retain that record, and any documents or

electronic files obtained electronically, in accordance with paragraph (o) of this section.

(5) Credit history evaluation. Licensees, applicants, contractors and vendors shall ensure that the full credit history of any individual who is applying for unescorted access or unescorted access authorization is evaluated. A full credit history evaluation must include, but is not limited to, an inquiry to detect potential fraud or misuse of social security numbers or other financial identifiers, and a review and evaluation of all of the information that is provided by a national credit-reporting agency about the individual's credit history. For individuals including foreign nationals and United States citizens who have resided outside the United States and do not have established credit history that covers at least the most recent seven years in the United States, the licensee, applicant, contractor or vendor must document all attempts to obtain information regarding the individual's credit history and financial responsibility from some relevant entity located in that other country or countries.

(6) Character and reputation evaluation. Licensees, applicants, contractors, and vendors shall ascertain the character and reputation of an individual who has applied for unescorted access or unescorted access authorization by conducting reference checks. Reference checks may not be conducted with any person who is known to be a close member of the individual's family, including but not limited to, the individual's spouse, parents, siblings, or children, or any individual who resides in the individual's permanent household. The reference checks must focus on the individual's reputation for trustworthiness and reliability.

(7) Criminal history review. The licensee's or applicant's reviewing official shall evaluate the entire criminal history record of an individual who is applying for unescorted access or unescorted access authorization to determine whether the individual has a record of criminal activity that may adversely impact his or her trustworthiness and reliability. A criminal history record must be obtained in accordance with the requirements of § 73.57. For individuals who do not have or are not expected to have unescorted access, a criminal history record of the

individual shall be obtained in accordance with the requirements set forth in paragraph (k)(1)(ii) of this section.

(e) Psychological assessment. In order to assist in determining an individual's trustworthiness and reliability, licensees, applicants, contractors or vendors shall ensure that a psychological assessment has been completed before the individual is granted unescorted access or certified unescorted access authorization. Individuals who are applying for initial unescorted access or unescorted access authorization, or who have not maintained unescorted access or unescorted access authorization for greater than 365 days, shall be subject to a psychological assessment. The psychological assessment must be designed to evaluate the possible adverse impact of any noted psychological characteristics on the individual's trustworthiness and reliability.

(1) A licensed psychologist or psychiatrist with the appropriate training and experience shall conduct the psychological assessment.

(2) The psychological assessment must be conducted in accordance with the applicable ethical principles for conducting such assessments established by the American Psychological Association or American Psychiatric Association.

(3) At a minimum, the psychological assessment must include the administration and interpretation of a standardized, objective, professionally-accepted psychological test that provides information to identify indications of disturbances in personality or psychopathology that may have adverse implications for an individual's trustworthiness and reliability. A psychiatrist or psychologist specified in paragraph (e) of this section shall establish the predetermined thresholds for each scale, in accordance with paragraph (e)(2) of this section, that must be applied in interpreting the results of the psychological test to determine whether an individual must be interviewed by a licensed psychiatrist or psychologist, under § 73.56(e)(4)(i) of this section.

(4) The psychological assessment must include a clinical interview:

(i) If an individual's scores on the psychological test in paragraph (e)(3) of this section identify indications of disturbances in personality or psychopathology that may have implications for an individual's trustworthiness and reliability; or

(ii) If the individual is a member of the population that performs one or more job functions that are critical to the safe and secure operation of the licensee's facility, as defined in paragraph (i)(1)(v)(B) of this section.

(5) In the course of conducting a psychological assessment for those individuals who are specified in paragraph (h) of this section for initial unescorted access or unescorted access authorization category, if the licensed psychologist or psychiatrist identifies or discovers any information, including a medical condition, that could adversely impact the individual's fitness for duty or trustworthiness and reliability, the licensee, applicant, or contractor or vendor shall ensure that the psychologist or psychiatrist contact appropriate medical personnel to obtain further information as need for a determination. The results of the evaluation and a recommendation shall be provided to the licensee's or applicant's reviewing official.

(6) During psychological reassessments, if the licensed psychologist or psychiatrist identifies or discovers any information, including a medical condition, that could adversely impact the fitness for duty or trustworthiness and reliability of those individuals who are currently granted unescorted access or certified unescorted access authorization status, he or she shall inform (1) the reviewing official of the discovery within 24 hours of the discovery and (2) the medical personnel designated in the site implementing procedures, who shall ensure that an appropriate evaluation of the possible medical condition is conducted under the requirements of part 26 of this chapter. The results of the evaluation and a recommendation shall be provided to the licensee's or applicant's reviewing official.

(f) Behavioral observation.

(1) Licensee and applicant access authorization programs must include a behavioral observation program that is designed to detect behaviors or activities that may constitute an unreasonable risk to the health and safety of the public and common defense and security, including a potential threat to commit radiological sabotage. Licensees, applicants and contractors or vendors must ensure that the individuals specified in paragraph (b)(1) and, if applicable, (b)(2) of this section are subject to behavioral observation.

(2) Each person subject to the behavior observation program shall be responsible for communicating to the licensee or applicant observed behaviors of individuals subject to the requirements of this section. Such behaviors include any behavior of individuals that may adversely affect the safety or security of the licensee's facility or that may constitute an unreasonable risk to the public health and safety or the common defense and security, including a potential threat to commit radiological sabotage.

(i) Licensees, applicants, and contractors or vendors shall ensure that individuals who are subject to this section also successfully complete initial behavioral observation training and requalification behavior observation training as required in paragraphs (f)(2)(ii) and (iii) of this section.

(ii) Behavioral observation training must be:

(A) Completed before the licensee grants unescorted access or certifies unescorted access authorization or an applicant certifies unescorted access authorization, as defined in paragraph (h)(4)(ii) of this section,

(B) Current before the licensee grants unescorted access update or reinstatement or licensee or applicant certifies unescorted access authorization reinstatement as defined in paragraph (h)(4)(ii) of this section, and

(C) Maintained in a current status during any period of time an individual possesses unescorted access or unescorted access authorization in accordance with paragraph (f)(2)(iv) of

this section.

(iii) For initial behavioral observation training, individuals shall demonstrate completion by passing a comprehensive examination that addresses the knowledge and abilities necessary to detect behavior or activities that have the potential to constitute an unreasonable risk to the health and safety of the public and common defense and security, including a potential threat to commit radiological sabotage. Remedial training and re-testing are required for individuals who fail to satisfactorily complete the examination.

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

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

(3) Individuals who are subject to an access authorization program under this section shall at a minimum, report any concerns arising from behavioral observation, including, but not limited to, concerns related to any questionable behavior patterns or activities of others to the reviewing official, his or her supervisor, or other management personnel designated in their site procedures. The recipient of the report shall, if other than the reviewing official, promptly convey the report to the reviewing official, who shall reassess the reported individual's unescorted access or unescorted access authorization status. The reviewing official shall determine the elements of the reassessment based on the accumulated information of the individual. If the reviewing official has a reason to believe that the reported individual's trustworthiness or reliability is questionable, the reviewing official shall either administratively withdraw or terminate the individual's unescorted access or unescorted access authorization while completing the re-

evaluation or investigation. If the reviewing official determines from the information provided that there is cause for additional action, the reviewing official may inform the supervisor of the reported individual.

(g) Self-reporting of legal actions.

(1) Any individual who has applied for unescorted access or unescorted access authorization or is maintaining unescorted access or unescorted access authorization under this section shall promptly report to the reviewing official, his or her supervisor, or other management personnel designated in site procedures any legal action(s) taken by a law enforcement authority or court of law to which the individual has been subject that could result in incarceration or a court order or that requires a court appearance, including but not limited to an arrest, an indictment, the filing of charges, or a conviction, but excluding minor civil actions or misdemeanors such as parking violations or speeding tickets. The recipient of the report shall, if other than the reviewing official, promptly convey the report to the reviewing official. On the day that the report is received, the reviewing official shall evaluate the circumstances related to the reported legal action(s) and re-determine the reported individual's unescorted access or unescorted access authorization status.

(2) The licensee or applicant shall inform the individual of this obligation, in writing, prior to granting unescorted access or certifying unescorted access authorization.

(h) Granting unescorted access and certifying unescorted access authorization. Licensees and applicants shall implement the requirements of this paragraph for granting or certifying initial or reinstated unescorted access or unescorted access authorization. The investigatory information collected to satisfy the requirements of this section for individuals who are being considered for unescorted access or unescorted access authorization shall be valid for a trustworthiness and reliability determination by a licensee or applicant for 30 calendar days.

(1) Determination basis.

(i) The licensee's or applicant's reviewing official shall determine whether to grant, certify, deny, unfavorably terminate, maintain, or administratively withdraw an individual's unescorted access or unescorted access authorization status, based on an evaluation of all of the information required by this section.

(ii) The licensee's or applicant's reviewing official may not grant unescorted access or certify unescorted access authorization status to an individual until all of the information required by this section has been evaluated by the reviewing official and the reviewing official has determined that the accumulated information supports a determination of the individual's trustworthiness and reliability. However, the reviewing official may deny or terminate unescorted access or unescorted access authorization of any individual based on disqualifying information even if not all the information required by this section has been collected or evaluated.

(2) Unescorted access for NRC-certified personnel. Licensees and applicants shall grant unescorted access to any individual who has been certified by the Nuclear Regulatory Commission as suitable for such access.

(3) Access denial. Licensees or applicants may not permit an individual, who is identified as having an access-denied status by another licensee subject to this section, or has an access authorization status other than favorably terminated, to enter any nuclear power plant protected area or vital area, under escort or otherwise, or take actions by electronic means that could adversely impact the licensee's or applicant's safety, security, or emergency response or their facilities, under supervision or otherwise, except upon completion of the initial unescorted access authorization process.

(4) Granting unescorted access and certifying unescorted access authorization.

(i) Initial unescorted access or unescorted access authorization. In satisfying the requirements of paragraph (h)(1) of this section, for individuals who have never held unescorted access or unescorted access authorization status or whose unescorted access or unescorted

access authorization status has been interrupted for a period of 3 years or more, the licensee, applicant, or contractor or vendor shall satisfy the requirements of paragraphs (d), (e), (f), and (g) of this section. In meeting requirements set forth in paragraph (d)(4) of this section, the licensee, applicant, or contractor or vendor shall evaluate the 3 years before the date on which the application for unescorted access was submitted, or since the individual's eighteenth birthday, whichever is shorter. For the 1-year period proceeding the date upon which the individual applies for unescorted access or unescorted access authorization, the licensee, applicant or contractor or vendor shall ensure that the employment history evaluation is conducted with every employer, regardless of the length of employment. For the remaining 2-year period, the licensee, applicant, or contractor or vendor shall ensure that the employment history evaluation is conducted with the employer by whom the individual claims to have been employed the longest within each calendar month.

(ii) Reinstatement of Unescorted Access. In satisfying the requirements of paragraph (h)(1) of this section, for individuals who have previously been granted unescorted access or unescorted access authorization, but whose access had been terminated under favorable conditions, licensees, applicants or contractors or vendors shall satisfy the requirements of paragraphs (d), (e), (f), and (g) of this section, with consideration of the specific requirements for periods of interruption described below in paragraphs (h)(4)(ii)(A) or (h)(4)(ii)(B) of this section, as applicable. However, for individuals whose unescorted access or unescorted access authorization was interrupted for less than or equal to 30 calendar days, licensees, applicants, or contractors or vendors must only satisfy the requirements set forth in paragraphs (d)(1), (d)(2), and (d)(3) of this section. The applicable periods of interruption are determined by the number of calendar days between the day after the individual's access was terminated and the day upon which the individual applies for unescorted access or unescorted access authorization.

(A) For individuals whose last unescorted access or unescorted access authorization

status has been interrupted for more than 30 calendar days but less than or equal to 365 calendar days, the licensee, applicant or contractor or vendor shall complete the individual's employment history evaluation in accordance with the requirements of paragraph (d)(4) of this section, within 5 business days after reinstatement. The licensee, applicant, or contractor or vendor shall ensure that the employment history evaluation has been conducted with the employer by whom the individual claims to have been employed the longest within the calendar month. However, if the employment history evaluation is not completed within 5 business days of reinstatement due to circumstances that are outside of the licensee's, applicant's, or contractor's or vendor's control and the licensee or applicant, contractor or vendor is not aware of any potentially disqualifying information regarding the individual within the past 5 years, the licensee may extend the individual's unescorted access an additional 5 business days. If the employment history evaluation is not completed within this extended 5 business days, the licensee shall administratively withdraw unescorted access and complete the employment history evaluation in accordance with § 73.56(d)(4) of this section. For re-certification of unescorted access authorization, prior to re-certification of unescorted access authorization status of an individual, the licensee or applicant shall complete all the elements stated above including drug screening and employment evaluation.

(B) For individuals whose last unescorted access or unescorted access authorization status has been interrupted for greater than 365 calendar days but fewer than 3 years the licensee, applicant or contractor or vendor shall evaluate the period of time since the individual last held unescorted access or unescorted access authorization status, up to and including the day the individual applies for re-instated unescorted access authorization. For the 1-year period proceeding the date upon which the individual applies for unescorted access authorization, the licensee, applicant, or contractor or vendor shall ensure that the employment history evaluation is conducted with every employer, regardless of the length of employment. For the remaining

period, the licensee, applicant or contractor or vendor shall ensure that the employment history evaluation is conducted with the employer by whom the individual claims to have been employed the longest within each calendar month. In addition, the individual shall be subject to the psychological assessment required in § 73.56(e).

(5) Accepting unescorted access authorization from other access authorization programs. Licensees who are seeking to grant unescorted access or certify unescorted access authorization or applicants who are seeking to certify unescorted access authorization to an individual who is subject to another access authorization program or another access authorization program that complies with this section may rely on those access authorization programs or access authorization program elements to comply with the requirements of this section. However, the licensee who is seeking to grant unescorted access or the licensee or applicant who is seeking to certify unescorted access authorization shall ensure that the program elements to be accepted have been maintained consistent with the requirements of this section by the other access authorization program.

(6) Information sharing. To meet the requirements of this section, licensees, applicants, and contractors or vendors may rely upon the information that other licensees, applicants, and contractors or vendors who are also subject to this section, have gathered about individuals who have previously applied for unescorted access or unescorted access authorization, and developed about individuals during periods in which the individuals maintained unescorted access or unescorted access authorization status.

(i) Maintaining unescorted access or unescorted access authorization

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

(i) The individual remains subject to a behavioral observation program that complies with the requirements of § 73.56(f) of this section.

(ii) The individual successfully completes behavioral observation refresher training or testing on the nominal 12-month frequency required in § 73.56(f)(2)(ii) of this section.

(iii) The individual complies with the licensee's or applicant's access authorization program policies and procedures to which he or she is subject, including the self-reporting of legal actions responsibility specified in paragraph (g) of this section.

(iv) The individual is subject to an annual supervisory review conducted in accordance with the requirements of the licensee's or applicant's behavioral observation program. The individual shall be subject to a supervisory interview in accordance with the requirements of the licensee's or applicant's behavioral observation program, if the supervisor does not have the frequent interaction with the individual throughout the review period needed to form an informed and reasonable opinion regarding the individual's behavior, trustworthiness, and reliability.

(v) The licensee's or applicant's reviewing official determines that the individual continues to be trustworthy and reliable. This determination must, at a minimum, be based on the following:

(A) A criminal history update and credit history re-evaluation for any individual with unescorted access. The criminal history update and credit history re-evaluation must be completed within 5 years of the date on which these elements were last completed.

(B) For individuals who perform one or more of the job functions described in this paragraph, the trustworthiness and reliability determination must be based on a criminal history update and credit history re-evaluation within three years of the date on which these elements were last completed, or more frequently, based on job assignment as determined by the licensee or applicant, and a psychological re-assessment within 5 years of the date on which this element was last completed:

(1) Individuals who have extensive knowledge of defensive strategies and design and/or implementation of the plant's defense strategies, including --

(i) Site security supervisors

(ii) Site security managers

(iii) Security training instructors and

(iv) Corporate security managers;

(2) Individuals in a position to grant an applicant unescorted access or unescorted access authorization, including site access authorization managers;

(3) Individuals assigned a duty to search for contraband or other items that could be used to commit radiological sabotage (i.e., weapons, explosives, incendiary devices);

(4) Individuals who have access, extensive knowledge, or administrative control over plant digital computer and communication systems and networks as identified in § 73.54, including --

(i) Plant network systems administrators;

(ii) IT personnel who are responsible for securing plant networks; or

(5) Individuals qualified for and assigned duties as: armed security officers, armed responders, alarm station operators, response team leaders, and armorers as defined in the licensee's or applicant's Physical Security Plan; and reactor operators, senior reactor operators and non-licensed operators. Non-licensed operators include those individuals responsible for the operation of plant systems and components, as directed by a reactor operator or senior reactor operator. A non-licensed operator also includes individuals who monitor plant instrumentation and equipment and principally perform their duties outside of the control room.

(C) The criminal history update and the credit history re-evaluation shall be completed

within 30 calendar days of each other.

(vi) If the criminal history update, credit history re-evaluation, psychological re-assessment, if required, and supervisory review and interview, if applicable, have not been completed and the information evaluated by the reviewing official within the time frame specified under paragraph (v) of this section, the licensee or applicant shall administratively withdraw the individual's unescorted access or unescorted access authorization until these requirements have been met.

(2) If an individual who has unescorted access or unescorted access authorization status is not subject to an access authorization program that meets the requirements of this part for more than 30 continuous days, then the licensee or applicant shall terminate the individual's unescorted access or unescorted access authorization status and the individual shall meet the requirements in this section, as applicable, to regain unescorted access or unescorted access authorization.

(j) Access to vital areas. Licensees or applicants shall establish, implement, and maintain a list of individuals who are authorized to have unescorted access to specific nuclear power plant vital areas during non-emergency conditions. The list must include only those individuals who have a continued need for access to those specific vital areas in order to perform their duties and responsibilities. The list must be approved by a cognizant licensee or applicant manager or supervisor who is responsible for directing the work activities of the individual who is granted unescorted access to each vital area, and updated and re-approved no less frequently than every 31 days.

(k) Trustworthiness and reliability of background screeners and access authorization program personnel. Licensees, applicants, and contractors or vendors shall ensure that any individual who collects, processes, or has access to personal information that is used to make unescorted access or unescorted access authorization determinations under this section has been determined to be trustworthy and reliable.

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

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

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

(iii) A credit history review and evaluation;

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

(v) An evaluation of character and reputation.

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

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

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

§ 73.56(k)(1)(ii) or a criminal history check that meets the requirements of § 73.56(d)(7).

(l) Review procedures. Each licensee and applicant shall include a procedure for the notification of individuals who are denied unescorted access, unescorted access authorization, or who are unfavorably terminated. Additionally, procedures must include provisions for the review, at the request of the affected individual, of a denial or unfavorable termination of unescorted access or unescorted access authorization that may adversely affect employment. The procedure must contain a provision to ensure the individual is informed of the grounds for the denial or unfavorable termination and allow the individual an opportunity to provide additional relevant information and an opportunity for an objective review of the information upon which the denial or unfavorable termination of unescorted access or unescorted access authorization was based. The procedure must provide for an impartial and independent internal management review. Licensees and applicants shall not grant unescorted access or certify unescorted access authorization, or permit the individual to maintain unescorted access or unescorted access authorization during the review process.

(m) Protection of information. Each licensee, applicant, contractor, or vendor shall establish and maintain a system of files and procedures to ensure personal information is not disclosed to unauthorized persons.

(1) Licensees, applicants and contractors or vendors shall obtain signed consent from the subject individual that authorizes the disclosure of any information collected and maintained under this section before disclosing the information, except for disclosures to the following individuals:

(i) The subject individual or his or her representative, when the individual has designated the representative in writing for specified unescorted access authorization matters;

(ii) NRC representatives;

(iii) Appropriate law enforcement officials under court order;

(iv) A licensee's, applicant's, or contractor's or vendor's representatives who have a need to have access to the information in performing assigned duties, including determinations of trustworthiness and reliability and audits of access authorization programs;

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

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

(vii) Other persons pursuant to court order.

(2) All information pertaining to a denial or unfavorable termination of the individual's unescorted access or unescorted access authorization shall be promptly provided, upon receipt of a written request by the subject individual or his or her designated representative as designated in writing. The licensee or applicant may redact the information to be released to the extent that personal privacy information, including the name of the source of the information is withheld.

(3) A contract with any individual or organization who collects and maintains personal information that is relevant to an unescorted access or unescorted access authorization determination must require that such records be held in confidence, except as provided in paragraphs (m)(1) through (m)(2) of this section.

(4) Licensees, applicants, or contractors or vendors and any individual or organization who collects and maintains personal information on behalf of a licensee, applicant, or contractor or vendor, shall establish, implement, and maintain a system and procedures for the secure storage and handling of the information collected.

(n) Audits and corrective action. Each licensee and applicant shall be responsible for the continuing effectiveness of the access authorization program, including access authorization program elements that are provided by the contractors or vendors, and the access authorization

programs of any the contractors or vendors that are accepted by the licensee or applicant. Each licensee, applicant, and contractor or vendor shall ensure that access authorization programs and program elements are audited to confirm compliance with the requirements of this section and those comprehensive actions are taken to correct any non-conformance that is identified.

(1) Each licensee and applicant shall ensure that its entire access authorization program is audited nominally every 24 months. Licensees, applicants and contractors or vendors are responsible for determining the appropriate frequency, scope, and depth of additional auditing activities within the nominal 24-month period based on the review of program performance indicators, such as the frequency, nature, and severity of discovered problems, personnel or procedural changes, and previous audit findings.

(2) Access authorization program services that are provided to a licensee or applicant by contractor or vendor personnel who are off site or are not under the direct daily supervision or observation of the licensee's or applicant's personnel must be audited by the licensee or applicant on a nominal 12-month frequency. In addition, any access authorization program services that are provided to contractors or vendors by subcontractor personnel who are off site or are not under the direct daily supervision or observation of the contractor's or vendor's personnel must be audited by the licensee or applicant on a nominal 12-month frequency.

(3) Licensee's and applicant's contracts with contractors or vendors must reserve the licensee's or applicant's right to audit the contractors or vendors and the contractor's or vendor's subcontractors providing access authorization program services at any time, including at unannounced times, as well as to review all information and documentation that is reasonably relevant to the performance of the program.

(4) Licensee's and applicant's contracts with the contactors or vendors, and contactors' or vendors' contracts with subcontractors, must also require that the licensee or applicant shall be provided access to and be permitted to take away copies of any documents or data that may be

needed to assure that the contractor or vendor and its subcontractors are performing their functions properly and that staff and procedures meet applicable requirements.

(5) Audits must focus on the effectiveness of the access authorization program or program element(s), as appropriate. At least one member of the licensee or applicant audit team shall be a person who is knowledgeable of and practiced with meeting the performance objectives and requirements of the access authorization program or program elements being audited. The individuals performing the audit of the access authorization program or program element(s) shall be independent from both the subject access authorization programs' management and from personnel who are directly responsible for implementing the access authorization program or program elements being audited.

(6) The results of the audits, along with any recommendations, must be documented in the site corrective action program in accordance with § 73.55(b)(10) and reported to senior management having responsibility in the area audited and to management responsible for the access authorization program. Each audit report must identify conditions that are adverse to the proper performance of the access authorization program, the cause of the condition(s), and, when appropriate, recommended corrective actions, and corrective actions taken. The licensee, applicant, or contractor or vendor shall review the audit findings and take any additional corrective actions, to include re-auditing of the deficient areas where indicated, to preclude repetition of the condition.

(7) Licensees and applicants may jointly conduct audits, or may accept audits of the contractors or vendors that were conducted by other licensees and applicants who are subject to this section, if the audit addresses the services obtained from the contractor or vendor by each of the sharing licensees and applicants. The contractors or vendors may jointly conduct audits, or may accept audits of its subcontractors that were conducted by other licensees, applicants, or contractors or vendors who are subject to this section, if the audit addresses the services

obtained from the subcontractor by each of the sharing licensees, applicants, and the contractors or vendors.

(i) Licensees, applicants, and contractors or vendors shall review audit records and reports to identify any areas that were not covered by the shared or accepted audit and ensure that authorization program elements and services upon which the licensee, applicant, or contractor or vendor relies are audited, if the program elements and services were not addressed in the shared audit.

(ii) Sharing licensees and applicants need not re-audit the same contractor or vendor for the same time. Sharing contractors or vendors need not re-audit the same subcontractor for the same time.

(iii) Sharing licensees, applicants, and contractors or vendors shall maintain a copy of the shared audits, including findings, recommendations, and corrective actions.

(o) Records. Licensee, applicants, and contractors or vendors shall maintain the records that are required by the regulations in this section for the period specified by the appropriate regulation. If a retention period is not otherwise specified, these records must be retained until the Commission terminates the facility's license, certificate, or other regulatory approval.

(1) Records may be stored and archived electronically, provided that the method used to create the electronic records meets the following criteria:

(i) Provides an accurate representation of the original records;

(ii) Prevents unauthorized access to the records;

(iii) Prevents the alteration of any archived information and/or data once it has been committed to storage; and

(iv) Permits easy retrieval and re-creation of the original records.

(2) Licensees and applicants who are subject to this section shall retain the following records:

(i) Records of the information that must be collected under paragraphs (d) and (e) of this section that results in the granting of unescorted access or certifying of unescorted access authorization for at least 5 years after the licensee or applicant terminates or denies an individual's unescorted access or unescorted access authorization or until the completion of all related legal proceedings, whichever is later;

(ii) Records pertaining to denial or unfavorable termination of unescorted access or unescorted access authorization and related management actions for at least 5 years after the licensee or applicant terminates or denies an individual's unescorted access or unescorted access authorization or until the completion of all related legal proceedings, whichever is later; and

(iii) Documentation of the granting and termination of unescorted access or unescorted access authorization for at least 5 years after the licensee or applicant terminates or denies an individual's unescorted access or unescorted access authorization or until the completion of all related legal proceedings, whichever is later. Contractors or vendors may maintain the records that are or were pertinent to granting, certifying, denying, or terminating unescorted access or unescorted access authorization that they collected for licensees or applicants. If the contractors or vendors maintain the records on behalf of a licensee or an applicant, they shall follow the record retention requirement specified in this section. Upon termination of a contract between the contractor and vendor and a licensee or applicant, the contractor or vendor shall provide the licensee or applicant with all records collected for the licensee or applicant under this chapter.

(3) Licensees, applicants, and contractors or vendors shall retain the following records for at least 3 years or until the completion of all related proceedings, whichever is later:

(i) Records of behavioral observation training conducted under paragraph (f)(2) of this section; and

(ii) Records of audits, audit findings, and corrective actions taken under paragraph (n) of this section.

(4) Licensees, applicants, and contractors or vendors shall retain written agreements for the provision of services under this section, for three years after termination or completion of the agreement, or until completion of all proceedings related to a denial or unfavorable termination of unescorted access or unescorted access authorization that involved those services, whichever is later.

(5) Licensees, applicants, and contractors or vendors shall retain records of the background investigations, psychological assessments, supervisory reviews, and behavior observation program actions related to access authorization program personnel, conducted under paragraphs (d) and (e) of this section, for the length of the individual's employment by or contractual relationship with the licensee, applicant, or the contractor or vendor and three years after the termination of employment, or until the completion of any proceedings relating to the actions of such access authorization program personnel, whichever is later.

(6) Licensees, applicants, and the contractors or vendors who have been authorized to add or manipulate data that is shared with licensees subject to this section shall ensure that data linked to the information about individuals who have applied for unescorted access or unescorted access authorization, which is specified in the licensee's or applicant's access authorization program documents, is retained.

(i) If the shared information used for determining individual's trustworthiness and reliability changes or new or additional information is developed about the individual, the licensees, applicants, and the contractors or vendors that acquire this information shall correct or augment the data and ensure it is shared with licensees subject to this section. If the changed, additional or developed information has implications for adversely affecting an individual's trustworthiness and reliability, the licensee, applicant, or the contractor or vendor

who discovered or obtained the new, additional or changed information, shall, on the day of discovery, inform the reviewing official of any licensee or applicant access authorization program under which the individual is maintaining his or her unescorted access or unescorted access authorization status of the updated information.

(ii) The reviewing official shall evaluate the shared information and take appropriate actions, which may include denial or unfavorable termination of the individual's unescorted access authorization. If the notification of change or updated information cannot be made through usual methods, licensees, applicants, and the contractors or vendors shall take manual actions to ensure that the information is shared as soon as reasonably possible. Records maintained in any database(s) must be available for NRC review.

(7) If a licensee or applicant administratively withdraws an individual's unescorted access or unescorted access authorization status caused by a delay in completing any portion of the background investigation or for a licensee or applicant initiated evaluation, or re-evaluation that is not under the individual's control, the licensee or applicant shall record this administrative action to withdraw the individual's unescorted access or unescorted access authorization with other licensees subject to this section. However, licensees and applicants shall not document this administrative withdrawal as denial or unfavorable termination and shall not respond to a suitable inquiry conducted under the provisions of 10 CFR parts 26, a background investigation conducted under the provisions of this section, or any other inquiry or investigation as denial nor unfavorable termination. Upon favorable completion of the background investigation element that caused the administrative withdrawal, the licensee or applicant shall immediately ensure that any matter that could link the individual to the administrative action is eliminated from the subject individual's access authorization or personnel record and other records, except if a review of the information obtained or developed causes the reviewing official to unfavorably terminate or deny the individual's unescorted access.

14. Section 73.58 is added to read as follows:

**§ 73.58 Safety/security interface requirements for nuclear power reactors**

(a) Each operating nuclear power reactor licensee with a license issued under part 50 or 52 of this chapter shall comply with the requirements of this section.

(b) The licensee shall assess and manage the potential for adverse effects on safety and security, including the site emergency plan, before implementing changes to plant configurations, facility conditions, or security.

(c) The scope of changes to be assessed and managed must include planned and emergent activities (such as, but not limited to, physical modifications, procedural changes, changes to operator actions or security assignments, maintenance activities, system reconfiguration, access modification or restrictions, and changes to the security plan and its implementation).

(d) Where potential conflicts are identified, the licensee shall communicate them to appropriate licensee personnel and take compensatory and/or mitigative actions to maintain safety and security under applicable Commission regulations, requirements, and license conditions.

15. In appendix B to part 73, section VI is added to the table of contents, the introduction text is revised by adding a new introductory paragraph, and section VI is added to read as follows:

**APPENDIX B TO PART 73-GENERAL CRITERIA FOR SECURITY PERSONNEL**

TABLE OF CONTENTS

* * * * *

VI. NUCLEAR POWER REACTOR TRAINING AND QUALIFICATION PLAN FOR PERSONNEL

PERFORMING SECURITY PROGRAM DUTIES

INTRODUCTION

Applicants and power reactor licensees subject to the requirements of § 73.55 shall comply only with the requirements of section VI of this appendix. All other licensees, applicants, or certificate holders shall comply only with sections I through V of this appendix.

* * * * *

## VI. NUCLEAR POWER REACTOR TRAINING AND QUALIFICATION PLAN FOR PERSONNEL PERFORMING SECURITY PROGRAM DUTIES

A. General Requirements and Introduction

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

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

3. The licensee shall establish, maintain, and follow a Commission-approved training and qualification plan, describing how the minimum training and qualification requirements set forth in this appendix will be met, to include the processes by which all individuals, will be

selected, trained, equipped, tested, and qualified.

4. Each individual assigned to perform security program duties and responsibilities required to effectively implement the Commission-approved security plans, licensee protective strategy, and the licensee implementing procedures, shall demonstrate the knowledge, skills, and abilities required to effectively perform the assigned duties and responsibilities before the individual is assigned the duty or responsibility.

5. The licensee shall ensure that the training and qualification program simulates, as closely as practicable, the specific conditions under which the individual shall be required to perform assigned duties and responsibilities.

6. The licensee may not allow any individual to perform any security function, assume any security duties or responsibilities, or return to security duty, until that individual satisfies the training and qualification requirements of this appendix and the Commission-approved training and qualification plan, unless specifically authorized by the Commission.

7. Annual requirements must be scheduled at a nominal twelve (12) month periodicity. Annual requirements may be completed up to three (3) months before or three (3) months after the scheduled date. However, the next annual training must be scheduled twelve (12) months from the previously scheduled date rather than the date the training was actually completed.

B. Employment suitability and qualification.

1. Suitability.

(a) Before employment, or assignment to the security organization, an individual shall:

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

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

(3) Not have any felony convictions that reflect on the individual's reliability.

(4) Individuals in an armed capacity, would not be disqualified from possessing or using firearms or ammunition in accordance with applicable state or Federal law, to include 18 U.S.C. 922. Licensees shall use information that has been obtained during the completion of the individual's background investigation for unescorted access to determine suitability. Satisfactory completion of a firearms background check for the individual under 10 CFR 73.19 of this part will also fulfill this requirement.

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

2. Physical qualifications.

(a) General physical qualifications.

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

(2) Armed and unarmed individuals assigned security duties and responsibilities shall be subject to a physical examination designed to measure the individual's physical ability to perform assigned duties and responsibilities as identified in the Commission-approved security plans, licensee protective strategy, and implementing procedures.

(3) This physical examination must be administered by a licensed health professional with the final determination being made by a licensed physician to verify the individual's physical capability to perform assigned duties and responsibilities.

(4) The licensee shall ensure that both armed and unarmed individuals who are assigned security duties and responsibilities identified in the Commission-approved security plans, the licensee protective strategy, and implementing procedures, meet the following

minimum physical requirements, as required to effectively perform their assigned duties.

(b) Vision.

(1) For each individual, distant visual acuity in each eye shall be correctable to 20/30 (Snellen or equivalent) in the better eye and 20/40 in the other eye with eyeglasses or contact lenses.

(2) Near visual acuity, corrected or uncorrected, shall be at least 20/40 in the better eye.

(3) Field of vision must be at least 70 degrees horizontal meridian in each eye.

(4) The ability to distinguish red, green, and yellow colors is required.

(5) Loss of vision in one eye is disqualifying.

(6) Glaucoma is disqualifying, unless controlled by acceptable medical or surgical means, provided that medications used for controlling glaucoma do not cause undesirable side effects which adversely affect the individual's ability to perform assigned security duties, and provided the visual acuity and field of vision requirements stated previously are met.

(7) On-the-job evaluation must be used for individuals who exhibit a mild color vision defect.

(8) If uncorrected distance vision is not at least 20/40 in the better eye, the individual shall carry an extra pair of corrective lenses in the event that the primaries are damaged. Corrective eyeglasses must be of the safety glass type.

(9) The use of corrective eyeglasses or contact lenses may not interfere with an individual's ability to effectively perform assigned duties and responsibilities during normal or emergency conditions.

(c) Hearing.

(1) Individuals may not have hearing loss in the better ear greater than 30 decibels average at 500 Hz, 1,000 Hz, and 2,000 Hz with no level greater that 40 decibels at any one frequency.

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

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

(d) Existing medical conditions.

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

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

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

(f) Other physical requirements. An individual who has been incapacitated due to a serious illness, injury, disease, or operation, which could interfere with the effective performance of assigned duties and responsibilities shall, before resumption of assigned duties and responsibilities, provide medical evidence of recovery and ability to perform these duties and responsibilities.

3. Psychological qualifications.

(a) Armed and unarmed individuals shall demonstrate the ability to apply good judgment, mental alertness, the capability to implement instructions and assigned tasks, and possess the

acuity of senses and ability of expression sufficient to permit accurate communication by written, spoken, audible, visible, or other signals required by assigned duties and responsibilities.

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

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

4. Medical examinations and physical fitness qualifications.

(a) Armed members of the security organization shall be subject to a medical examination by a licensed physician, to determine the individual's fitness to participate in physical fitness tests.

(1) The licensee shall obtain and retain a written certification from the licensed physician that no medical conditions were disclosed by the medical examination that would preclude the individual's ability to participate in the physical fitness tests or meet the physical fitness attributes or objectives associated with assigned duties.

(b) Before assignment, armed members of the security organization shall demonstrate physical fitness for assigned duties and responsibilities by performing a practical physical fitness test.

(1) The physical fitness test must consider physical conditions such as strenuous activity, physical exertion, levels of stress, and exposure to the elements as they pertain to each individual's assigned security duties for both normal and emergency operations and must

simulate site specific conditions under which the individual will be required to perform assigned duties and responsibilities.

(2) The licensee shall describe the physical fitness test in the Commission-approved training and qualification plan.

(3) The physical fitness test must include physical attributes and performance objectives which demonstrate the strength, endurance, and agility, consistent with assigned duties in the Commission-approved security plans, licensee protective strategy, and implementing procedures during normal and emergency conditions.

(4) The physical fitness qualification of each armed member of the security organization must be documented by a qualified training instructor and attested to by a security supervisor.

5. Physical requalification.

(a) At least annually, armed and unarmed individuals shall be required to demonstrate the capability to meet the physical requirements of this appendix and the licensee training and qualification plan.

(b) The physical requalification of each armed and unarmed individual must be documented by a qualified training instructor and attested to by a security supervisor.

C. Duty training.

1. Duty training and qualification requirements. All personnel who are assigned to perform any security-related duty or responsibility shall be trained and qualified to perform assigned duties and responsibilities to ensure that each individual possesses the minimum knowledge, skills, and abilities required to effectively carry out those assigned duties and responsibilities.

(a) The areas of knowledge, skills, and abilities that are required to perform assigned duties and responsibilities must be identified in the licensee's Commission-approved training and qualification plan.

(b) Each individual who is assigned duties and responsibilities identified in the Commission-approved security plans, licensee protective strategy, and implementing procedures shall, before assignment:

(1) Be trained to perform assigned duties and responsibilities in accordance with the requirements of this appendix and the Commission-approved training and qualification plan.

(2) Meet the minimum qualification requirements of this appendix and the Commission-approved training and qualification plan.

(3) Be trained and qualified in the use of all equipment or devices required to effectively perform all assigned duties and responsibilities.

2. On-the-job training.

(a) The licensee training and qualification program must include on-the-job training performance standards and criteria to ensure that each individual demonstrates the requisite knowledge, skills, and abilities needed to effectively carry-out assigned duties and responsibilities in accordance with the Commission-approved security plans, licensee protective strategy, and implementing procedures, before the individual is assigned the duty or responsibility.

(b) In addition to meeting the requirement stated in paragraph C.2.(a) of this appendix, before assignment, individuals (e.g. response team leaders, alarm station operators, armed responders, and armed security officers designated as a component of the protective strategy) assigned duties and responsibilities to implement the Safeguards Contingency Plan shall complete a minimum of 40 hours of on-the-job training to demonstrate their ability to effectively apply the knowledge, skills, and abilities required to effectively perform assigned <u>contingency</u> duties and responsibilities in accordance with the approved safeguards contingency plan, other security plans, licensee protective strategy, and implementing procedures. On-the-job training must be documented by a qualified training instructor and attested to by a security supervisor.

(c) On-the-job training for contingency activities and drills must include, but is not limited to, hands-on application of knowledge, skills, and abilities related to:

(1) Response team duties.

(2) Use of force.

(3) Tactical movement.

(4) Cover and concealment.

(5) Defensive positions.

(6) Fields-of-fire.

(7) Re-deployment.

(8) Communications (primary and alternate).

(9) Use of assigned equipment.

(10) Target sets.

(11) Table top drills.

(12) Command and control duties.

(13) Licensee Protective Strategy.

3. Performance Evaluation Program.

(a) Licensees shall develop, implement and maintain a Performance Evaluation Program that is documented in procedures which describes how the licensee will demonstrate and assess the effectiveness of their onsite physical protection program and protective strategy, including the capability of the armed response team to carry out their assigned duties and responsibilities during safeguards contingency events. The Performance Evaluation Program and procedures shall be referenced in the licensee's Training and Qualifications Plan.

(b) The Performance Evaluation Program shall include procedures for the conduct of tactical response drills and force-on-force exercises designed to demonstrate and assess the effectiveness of the licensee's physical protection program, protective strategy and contingency

event response by all individuals with responsibilities for implementing the safeguards contingency plan.

(c) The licensee shall conduct tactical response drills and force-on-force exercises in accordance with Commission-approved security plans, licensee protective strategy, and implementing procedures.

(d) Tactical response drills and force-on-force exercises must be designed to challenge the site protective strategy against elements of the design basis threat and ensure each participant assigned security duties and responsibilities identified in the Commission-approved security plans, the licensee protective strategy, and implementing procedures demonstrate the requisite knowledge, skills, and abilities.

(e) Tactical response drills, force-on-force exercises, and associated contingency response training shall be conducted under conditions that simulate, as closely as practicable, the site-specific conditions under which each member will, or may be, required to perform assigned duties and responsibilities.

(f) The scope of tactical response drills conducted for training purposes shall be determined by the licensee and must address site-specific, individual or programmatic elements, and may be limited to specific portions of the site protective strategy.

(g) Each tactical response drill and force-on-force exercise shall include a documented post-exercise critique in which participants identify failures, deficiencies or other findings in performance, plans, equipment or strategies.

(h) Licensees shall document scenarios and participants for all tactical response drills and annual force-on-force exercises conducted.

(i) Findings, deficiencies and failures identified during tactical response drills and force-on-force exercises that adversely affect or decrease the effectiveness of the protective strategy and physical protection program shall be entered into the licensee's corrective action program to

ensure that timely corrections are made to the appropriate program areas.

(j) Findings, deficiencies and failures associated with the onsite physical protection program and protective strategy shall be protected as necessary in accordance with the requirements of 10 CFR 73.21.

(k) For the purpose of tactical response drills and force-on-force exercises, licensees shall:

(1) Use no more than the total number of armed responders and armed security officers documented in the security plans.

(2) Minimize the number and effects of artificialities associated with tactical response drills and force-on-force exercises.

(3) Implement the use of systems or methodologies that simulate the realities of armed engagement through visual and audible means, and reflect the capabilities of armed personnel to neutralize a target though the use of firearms.

(4) Ensure that each scenario used provides a credible, realistic challenge to the protective strategy and the capabilities of the security response organization.

(l) The Performance Evaluation Program must be designed to ensure that:

(1) Each member of each shift who is assigned duties and responsibilities required to implement the safeguards contingency plan and licensee protective strategy participates in at least one (1) tactical response drill on a quarterly basis and one (1) force-on-force exercise on an annual basis. Force-on-force exercises conducted to satisfy the NRC triennial evaluation requirement can be used to satisfy the annual force-on-force requirement for the personnel that participate in the capacity of the security response organization.

(2) The mock adversary force replicates, as closely as possible, adversary characteristics and capabilities of the design basis threat described in 10 CFR 73.1(a)(1), and is capable of exploiting and challenging the licensees protective strategy, personnel, command and control,

and implementing procedures.

(3) Protective strategies can be evaluated and challenged through the conduct of tactical response tabletop demonstrations.

(4) Drill and exercise controllers are trained and qualified to ensure that each controller has the requisite knowledge and experience to control and evaluate exercises.

(5) Tactical response drills and force-on-force exercises are conducted safely and in accordance with site safety plans.

(m) Scenarios.

(1) Licensees shall develop and document multiple scenarios for use in conducting quarterly tactical response drills and annual force-on-force exercises.

(2) Licensee scenarios must be designed to test and challenge any components or combination of components, of the onsite physical protection program and protective strategy.

(3) Each scenario must use a unique target set or target sets, and varying combinations of adversary equipment, strategies, and tactics, to ensure that the combination of all scenarios challenges every component of the onsite physical protection program and protective strategy to include, but not limited to, equipment, implementing procedures, and personnel.

D. Duty qualification and requalification.

1. Qualification demonstration.

(a) Armed and unarmed individuals shall demonstrate the required knowledge, skills, and abilities to carry out assigned duties and responsibilities as stated in the Commission-approved security plans, licensee protective strategy, and implementing procedures.

(b) This demonstration must include written exams and hands-on performance demonstrations.

(1) Written Exams. The written exams must include those elements listed in the Commission-approved training and qualification plan and shall require a minimum score of 80

percent to demonstrate an acceptable understanding of assigned duties and responsibilities, to include the recognition of potential tampering involving both safety and security equipment and systems.

(2) Hands-on Performance Demonstrations. Armed and unarmed individuals shall demonstrate hands-on performance for assigned duties and responsibilities by performing a practical hands-on demonstration for required tasks. The hands-on demonstration must ensure that theory and associated learning objectives for each required task are considered and each individual demonstrates the knowledge, skills, and abilities required to effectively perform the task.

(3) Annual Written Exam. Armed individuals shall be administered an annual written exam that demonstrates the required knowledge, skills, and abilities to carry out assigned duties and responsibilities as an armed member of the security organization. The annual written exam must include those elements listed in the Commission-approved training and qualification plan and shall require a minimum score of 80 percent to demonstrate an acceptable understanding of assigned duties and responsibilities.

(c) Upon request by an authorized representative of the Commission, any individual assigned to perform any security-related duty or responsibility shall demonstrate the required knowledge, skills, and abilities for each assigned duty and responsibility, as stated in the Commission-approved security plans, licensee protective strategy, or implementing procedures.

2. Requalification.

(a) Armed and unarmed individuals shall be requalified at least annually in accordance with the requirements of this appendix and the Commission-approved training and qualification plan.

(b) The results of requalification must be documented by a qualified training instructor and attested by a security supervisor.

E. Weapons training.

1. General firearms training.

(a) Armed members of the security organization shall be trained and qualified in accordance with the requirements of this appendix and the Commission-approved training and qualification plan.

(b) Firearms instructors.

(1) Each armed member of the security organization shall be trained and qualified by a certified firearms instructor for the use and maintenance of each assigned weapon to include but not limited to, marksmanship, assembly, disassembly, cleaning, storage, handling, clearing, loading, unloading, and reloading, for each assigned weapon.

(2) Firearms instructors shall be certified from a national or state recognized entity.

(3) Certification must specify the weapon or weapon type(s) for which the instructor is qualified to teach.

(4) Firearms instructors shall be recertified in accordance with the standards recognized by the certifying national or state entity, but in no case shall recertification exceed three (3) years.

(c) Annual firearms familiarization. The licensee shall conduct annual firearms familiarization training in accordance with the Commission-approved training and qualification plan.

(d) The Commission-approved training and qualification plan shall include, but is not limited to, the following areas:

(1) Mechanical assembly, disassembly, weapons capabilities and fundamentals of marksmanship.

(2) Weapons cleaning and storage.

(3) Combat firing, day and night.

(4) Safe weapons handling.

(5) Clearing, loading, unloading, and reloading.

(6) Firing under stress.

(7) Zeroing duty weapon(s) and weapons sighting adjustments.

(8) Target identification and engagement.

(9) Weapon malfunctions.

(10) Cover and concealment.

(11) Weapon familiarization.

(e) The licensee shall ensure that each armed member of the security organization is instructed on the use of deadly force as authorized by applicable state law.

(f) Armed members of the security organization shall participate in weapons range activities on a nominal four (4) month periodicity. Performance may be conducted up to five (5) weeks before to five (5) weeks after the scheduled date. The next scheduled date must be four (4) months from the originally scheduled date.

F. Weapons qualification and requalification program.

1. General weapons qualification requirements.

(a) Qualification firing must be accomplished in accordance with Commission requirements and the Commission-approved training and qualification plan for assigned weapons.

(b) The results of weapons qualification and requalification must be documented and retained as a record.

2. Tactical weapons qualification. The licensee Training and Qualification Plan must describe the firearms used, the firearms qualification program, and other tactical training required to implement the Commission-approved security plans, licensee protective strategy, and implementing procedures. Licensee developed tactical qualification and re-qualification

courses must describe the performance criteria needed to include the site specific conditions (such as lighting, elevation, fields-of-fire) under which assigned personnel shall be required to carry-out their assigned duties.

3. Firearms qualification courses. The licensee shall conduct the following qualification courses for each weapon used.

(a) Annual daylight qualification course. Qualifying score must be an accumulated total of 70 percent with handgun and shotgun, and 80 percent with semi-automatic rifle and/or enhanced weapons, of the maximum obtainable target score.

(b) Annual night fire qualification course. Qualifying score must be an accumulated total of 70 percent with handgun and shotgun, and 80 percent with semi-automatic rifle and/or enhanced weapons, of the maximum obtainable target score.

(c) Annual tactical qualification course. Qualifying score must be an accumulated total of 80 percent of the maximum obtainable score.

4. Courses of fire.

(a) Handgun. Armed members of the security organization, assigned duties and responsibilities involving the use of a revolver or semiautomatic pistol shall qualify in accordance with standards established by a law enforcement course, or an equivalent nationally recognized course.

(b) Semiautomatic rifle. Armed members of the security organization, assigned duties and responsibilities involving the use of a semiautomatic rifle shall qualify in accordance with the standards established by a law enforcement course, or an equivalent nationally recognized course.

(c) Shotgun. Armed members of the security organization, assigned duties and responsibilities involving the use of a shotgun shall qualify in accordance with standards established by a law enforcement course, or an equivalent nationally recognized course.

(d) Enhanced weapons. Armed members of the security organization, assigned duties and responsibilities involving the use of any weapon or weapons not described previously shall qualify in accordance with applicable standards established by a law enforcement course or an equivalent nationally recognized course for these weapons.

5. Firearms requalification.

(a) Armed members of the security organization shall be re-qualified for each assigned weapon at least annually in accordance with Commission requirements and the Commission-approved training and qualification plan, and the results documented and retained as a record.

(b) Firearms requalification must be conducted using the courses of fire outlined in paragraphs F.2, F.3, and F.4 of this section.

G. Weapons, personal equipment and maintenance.

1. Weapons. The licensee shall provide armed personnel with weapons that are capable of performing the function stated in the Commission-approved security plans, licensee protective strategy, and implementing procedures.

2. Personal equipment.

(a) The licensee shall ensure that each individual is equipped or has ready access to all personal equipment or devices required for the effective implementation of the Commission-approved security plans, licensee protective strategy, and implementing procedures.

(b) The licensee shall provide armed security personnel, required for the effective implementation of the Commission-approved Safeguards Contingency Plan and implementing procedures, at a minimum, but is not limited to, the following**:**

(1) Gas mask, full face.

(2) Body armor (bullet-resistant vest).

(3) Ammunition/equipment belt.

(4) Two-way portable radios, 2 channels minimum, 1 operating and 1 emergency.

(c) Based upon the licensee protective strategy and the specific duties and responsibilities assigned to each individual, the licensee should provide, as appropriate, but is not limited to, the following.

(1) Flashlights and batteries.

(2) Baton or other non-lethal weapons.

(3) Handcuffs.

(4) Binoculars.

(5) Night vision aids (e.g., goggles, weapons sights).

(6) Hand-fired illumination flares or equivalent.

(7) Duress alarms.

3. Maintenance.

(a) Firearms maintenance program. Each licensee shall implement a firearms maintenance and accountability program in accordance with the Commission regulations and the Commission-approved training and qualification plan. The program must include:

(1) Semiannual test firing for accuracy and functionality.

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

(3) Program activity documentation.

(4) Control and accountability (weapons and ammunition).

(5) Firearm storage requirements.

(6) Armorer certification.

H. Records.

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

2. The licensee shall retain each individual's initial qualification record for three (3) years

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

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

I. Reviews. The licensee shall review the Commission-approved training and qualification program in accordance with the requirements of § 73.55(n).

J. Definitions. Terms defined in parts 50, 70, and 73 of this chapter have the same meaning when used in this appendix.

16. In appendix C to part 73, a heading for section I and a new introductory paragraph are added before the "Introductory" section, and section II is added at the end of the appendix to read as follows:

**APPENDIX C TO PART 73 - NUCLEAR POWER PLANT SAFEGUARDS CONTINGENCY PLANS**.

I. **Safeguards Contingency Plan**

Licensee, applicants, and certificate holders, with the exception of those who are subject to the requirements of § 73.55 shall comply with the requirements of this section.

* * * * *

II. **Nuclear Power Plant Safeguards Contingency Plans**

A. Introduction.

The safeguards contingency plan is a documented plan that describes how licensee personnel implement their physical protection program to defend against threats to their facility, up to and including the design basis threat of radiological sabotage. The goals of licensee safeguards contingency plans are:

(1) To organize the response effort at the licensee level;

(2) To provide predetermined, structured response by licensees to safeguards contingencies;

(3) To ensure the integration of the licensee response by other entities; and

(4) To achieve a measurable performance in response capability.

Licensee safeguards contingency planning should result in organizing the licensee's resources in such a way that the participants will be identified, their responsibilities specified, and the responses coordinated. The responses should be timely, and include personnel who are trained and qualified to respond in accordance with a documented training and qualification program.

The evaluation, validation, and testing of this portion of the program shall be conducted in accordance with appendix B of this part, General Criteria for Security Personnel. The licensee's safeguards contingency plan is intended to maintain effectiveness during the implementation of emergency plans developed under appendix E to part 50 of this chapter.

B. Contents of the plan.

Each safeguards contingency plan shall include five (5) categories of information:

(1) Background.

(2) Generic planning base.

(3) Licensee planning base.

(4) Responsibility matrix.

(5) Implementing procedures.

Although the implementing procedures (the fifth category of plan information) are the culmination of the planning process, and are an integral and important part of the safeguards contingency plan, they entail operating details subject to frequent changes. They need not be submitted to the Commission for approval, but are subject to inspection by NRC staff on a

periodic basis.

1. Background. This category of information shall identify the perceived dangers and incidents that the plan will address and a general description of how the response is organized.

a. Perceived Danger - Consistent with the design basis threat specified in § 73.1(a)(1), licensees shall identify and describe the perceived dangers, threats, and incidents against which the safeguards contingency plan is designed to protect.

b. Purpose of the Plan - Licensees shall describe the general goals, objectives and operational concepts underlying the implementation of the approved safeguards contingency plan.

c. Scope of the Plan - A delineation of the types of incidents covered by the plan.

(i) How the onsite response effort is organized and coordinated to effectively respond to a safeguards contingency event.

(ii) How the onsite response for safeguards contingency events has been integrated in other site emergency response procedures.

d. Definitions - A list of terms and their definitions used in describing operational and technical aspects of the approved safeguards contingency plan.

2. Generic Planning Base. Licensees shall define the criteria for initiation and termination of responses to security events to include the specific decisions, actions, and supporting information needed to respond to each type of incident covered by the approved safeguards contingency plan. To achieve this result the generic planning base must:

a. Identify those events that will be used for signaling the beginning or aggravation of a safeguards contingency event according to how they are perceived initially by licensee's personnel. Licensees shall ensure detection of unauthorized activities and shall respond to all alarms or other indications signaling a security event, such as penetration of a protected area, vital area, or unauthorized barrier penetration (vehicle or personnel); tampering, bomb threats, or

other threat warnings - either verbal, such as telephoned threats, or implied, such as escalating civil disturbances.

b. Define the specific objective to be accomplished relative to each identified safeguards contingency event. The objective may be to obtain a level of awareness about the nature and severity of the safeguards contingency to prepare for further responses; to establish a level of response preparedness; or to successfully nullify or reduce any adverse safeguards consequences arising from the contingency.

c. Identify the data, criteria, procedures, mechanisms and logistical support necessary to achieve the objectives identified.

3. Licensee Planning Base. This category of information shall include factors affecting safeguards contingency planning that are specific for each facility. To the extent that the topics are treated in adequate detail in the licensee's approved physical security plan, they may be incorporated by reference in the Safeguards Contingency Plan. The following topics must be addressed:

a. Organizational Structure. The safeguards contingency plan must describe the organization's chain of command and delegation of authority during safeguards contingency events, to include a general description of how command and control functions will be coordinated and maintained.

b. Physical Layout. The safeguards contingency plan must include a site map depicting the physical structures located on the site, including onsite independent spent fuel storage installations, and a description of the structures depicted on the map. Plans must also include a description and map of the site in relation to nearby towns, transportation routes (e.g., rail, water, and roads), pipelines, airports, hazardous material facilities, and pertinent environmental features that may have an effect upon coordination of response activities. Descriptions and maps must indicate main and alternate entry routes for law enforcement or other offsite response and

support agencies and the location for marshaling and coordinating response activities.

c. Safeguards Systems. The safeguards contingency plan must include a description of the physical security systems that support and influence how the licensee will respond to an event in accordance with the design basis threat described in § 73.1(a). The licensee's description shall begin with onsite physical protection measures implemented at the outermost facility perimeter, and must move inward through those measures implemented to protect target set equipment.

(i) Physical security systems and security systems hardware to be discussed include security systems and measures that provide defense in depth, such as physical barriers, alarm systems, locks, area access, armaments, surveillance, and communications systems.

(ii) The specific structure of the security response organization to include the total number of armed responders and armed security officers documented in the approved security plans as a component of the protective strategy and a general description of response capabilities shall also be included the safeguards contingency plan.

(iii) Licensees shall ensure that individuals assigned duties and responsibilities to implement the safeguards contingency plan are trained and qualified in those duties according to the Commission approved security plans, training and qualification plans, and the performance evaluation program.

(iv) Armed responders shall be available to respond from designated areas inside the protected area at all times and may not be assigned any other duties or responsibilities that could interfere with assigned armed response team duties and responsibilities.

(v) Licensees shall develop, implement, and maintain a written protective strategy to be documented in procedures that describe in detail the physical protection measures, security systems and deployment of the armed response team relative to site specific conditions, to include but not limited to, facility layout, and the location of target set equipment and elements.

The protective strategy should support the general goals, operational concepts, and performance objectives identified in the licensee's safeguards contingency plan. The protective strategy shall:

(1) Be designed to meet the performance objectives of § 73.55(a) through (k).

(2) Identify predetermined actions, areas of responsibility and timelines for the deployment of armed personnel.

(3) Contain measures that limit the exposure of security personnel to possible attack, including incorporation of bullet resisting protected positions.

(4) Contain a description of the physical security systems and measures that provide defense in depth such as physical barriers, alarm systems, locks, area access, armaments, surveillance, and communications systems.

(5) Describe the specific structure and responsibilities of the armed response organization to include:

The authorized minimum number of armed responders, available at all times inside the protected area.

The authorized minimum number of armed security officers, available onsite at all times.

The total number of armed responders and armed security officers documented in the approved security plans as a component of the protective strategy.

(6) Provide a command and control structure, to include response by off-site law enforcement agencies, which ensures that decisions and actions are coordinated and communicated in a timely manner to facilitate response.

d. Law Enforcement Assistance. Provide a listing of available law enforcement agencies and a general description of their response capabilities and their criteria for response and a discussion of working agreements or arrangements for communicating with these agencies.

e. Policy Constraints and Assumptions.

The safeguards contingency plan shall contain a discussion of State laws, local

ordinances, and company policies and practices that govern licensee response to incidents and must include, but is not limited to, the following.

(i) Use of deadly force.

(ii) Recall of off-duty employees.

(iii) Site jurisdictional boundaries.

(iv) Use of enhanced weapons, if applicable.

f. Administrative and Logistical Considerations. Descriptions of licensee practices which influence how the security organization responds to a safeguards contingency event to include, but not limited to, a description of the procedures that will be used for ensuring that equipment needed to facilitate response will be readily accessible, in good working order, and in sufficient supply.

4. Responsibility Matrix. This category of information consists of the detailed identification of responsibilities and specific actions to be taken by licensee organizations and/or personnel in response to safeguards contingency events.

a. Licensees shall develop site procedures that consist of matrixes detailing the organization and/or personnel responsible for decisions and actions associated with specific responses to safeguards contingency events. The responsibility matrix and procedures shall be referenced in the licensee's safeguards contingency plan.

b. Responsibility matrix procedures shall be based on the events outlined in the licensee's Generic Planning Base and must include the following information:

(i) The definition of the specific objective to be accomplished relative to each identified safeguards contingency event. The objective may be to obtain a level of awareness about the nature and severity of the safeguards contingency to prepare for further responses, to establish a level of response preparedness, or to successfully nullify or reduce any adverse safeguards consequences arising from the contingency.

(ii) A tabulation for each identified initiating event and each response entity which depicts the assignment of responsibilities for decisions and actions to be taken in response to the initiating event.

(iii) An overall description of response actions and interrelationships specifically associated with each responsible entity must be included.

c. Responsibilities shall be assigned in a manner that precludes conflict of duties and responsibilities that would prevent the execution of the safeguards contingency plan and emergency response plans.

d. Licensees shall ensure that predetermined actions can be completed under the postulated conditions.

5. Implementing Procedures.

(i) Licensees shall establish and maintain written implementing procedures that provide specific guidance and operating details that identify the actions to be taken and decisions to be made by each member of the security organization who is assigned duties and responsibilities required for the effective implementation of the security plans and the site protective strategy.

(ii) Licensees shall ensure that implementing procedures accurately reflect the information contained in the Responsibility Matrix required by this appendix, the security plans, and other site plans.

(iii) Implementing procedures need not be submitted to the Commission for approval but are subject to inspection.

C. Records and reviews.

1. Licensees shall review the safeguards contingency plan in accordance with the requirements of § 73.55 (n).

2. The safeguards contingency plan audit must include a review of applicable elements of the Physical Security Plan, Training and Qualification Plan, implementing procedures and

practices, the site protective strategy, and response agreements made by local, State, and Federal law enforcement authorities.

3. Licensees shall retain all reports, records, or other documentation required by this appendix in accordance with the requirements of § 73.55.

Dated at Rockville, Maryland, this _____ day of _____ 2008.

For the Nuclear Regulatory Commission.

Annette L. Vietti-Cook,
Secretary of the Commission.