RULEMAKING ISSUE
(Notation Vote)

July 9, 2008 SECY-08-0099

FOR: The Commissioners

FROM: R. W. Borchardt
Executive Director for Operations

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

PURPOSE:

To request Commission approval for publication of the final rule.

SUMMARY:

The Nuclear Regulatory Commission (NRC) staff is recommending that the Commission amend its regulations governing security requirements for nuclear power plants. This final rule would amend existing security regulations and add new security requirements pertaining to current and future nuclear power reactors. This final rule would make security requirements similar to those previously imposed by the Commission orders issued after the terrorist attacks of September 11, 2001, generically applicable. Additionally, this final rule would add several new requirements developed as a result of insights gained from implementation of the security orders, reviews of site security plans, implementation of the enhanced baseline inspection program, and NRC evaluation of force-on-force exercises. The final rule would also update the NRC's security regulatory framework for the licensing of new nuclear power plants. Finally, three petitions for rulemaking (PRM) were considered during the development of the final rule requirements, consistent with the previous petition resolution and closure process for these petitions (PRM-50-80, PRM-73-11, and PRM-73-13).

CONTACTS: Bonnie Schnetzler, NSIR/DSP
(301) 415-7883

Timothy Reed, NRR/DPR
(301) 415-1462

BACKGROUND:

The basis for this rulemaking has been derived from several sources. First, prior to the events of September 11, 2001, the NRC had already undertaken an effort to revise its existing security regulations in 10 CFR Part 73, as noted in SECY-01-0101 (June 4, 2001). The existing security regulations in Part 73 have not been substantially revised for nearly 30 years. After September 11, 2001, that rulemaking effort was delayed for obvious reasons, but the need to reorganize, improve, and update the existing security regulations persists. This rulemaking built upon the efforts of the prior rulemaking.

Second, following the terrorist attacks on September 11, 2001, the NRC conducted a thorough review of security requirements to ensure that nuclear power plants and other licensed facilities continued to have effective security measures in place given the changing threat environment. Through a series of orders, the Commission supplemented the design basis threat (DBT) as well as established new requirements for specific training enhancements, access authorization enhancements, and enhancements to defensive strategies, mitigative measures, and integrated response. The following four security orders were issued to power reactor licensees:

- EA-02-026, “Interim Compensatory Measures Order,” issued February 25, 2002;
- EA-02-261, “Access Authorization Order,” issued January 7, 2003;
- EA-03-039, “Security Personnel Training and Qualification Requirements Order,” issued April 29, 2003; and
- EA-03-086, “Revised Design Basis Threat Order,” issued April 29, 2003.

While the specific’s of the orders are protected as Safeguards Information (SGI), in general, the enhancements resulted in such measures as increased patrols; augmented security forces and force capabilities; additional security posts; additional physical barriers; vehicle checks at greater standoff distances; enhanced coordination with law enforcement and military 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. Nuclear power plant licensees revised their site-specific physical security plans, access authorization programs, training and qualification plans, and safeguards contingency plans in response to these orders. The NRC completed its review and approval of all of these revised security plans on October 29, 2004.

Finally, 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, which added Section 161A to the Atomic Energy Act of 1954, as amended (AEA), concerns use of an expanded arsenal of weapons including machine guns and semi-automatic assault weapons by NRC licensees as well as imposing certain requirements for fingerprint-based firearms background checks. As noted below, because of considerations that have arisen during the course of this rulemaking, the final rule no longer specifically addresses any provisions of the EPAct 2005.

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

imposed on licensees by the various orders, the proposed rule also contains several new provisions that the NRC determined would provide additional assurance of licensees' capabilities to protect against the DBT. These new provisions were identified during implementation of the security orders while reviewing the revised site security plans that had been submitted by licensees for NRC 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, safety/security interface, central and secondary alarm stations functional equivalency, uninterruptable backup power for detection and assessment equipment, and real-time play-back video image equipment (October 26, 2006; 71 FR 62666-62667).

STAKEHOLDER INTERACTION:

Recipients of the post-September 11, 2001, orders were notified that the requirements in those orders were considered interim measures and that the NRC ultimately intended to reassess those requirements and undertake a rulemaking that would codify generically-applicable security requirements and revise the Commission's existing security regulations. To that end, on October 26, 2006 (71 FR 62664), the Commission published the proposed Power Reactor Security Rulemaking in the *Federal Register*. The proposed rule was originally published for a 75-day public comment period. However, in response to several requests for extension, the comment period was extended on two separate occasions (January 5, 2007; 72 FR 480; and February 28, 2007; 72 FR 8951), eventually closing on March 26, 2007. The NRC received 48 comment letters. In addition, the NRC staff held two public meetings to solicit public comment in Rockville, Maryland, on November 15, 2006, and in Las Vegas, Nevada, on November 29, 2006. The NRC staff also held a third public meeting in Rockville, Maryland, on March 9, 2007, to facilitate stakeholder understanding of the proposed requirements and thereby result in more informed comment on the proposed rule.

The NRC 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 staff wished to provide additional clarifying rule language. The supplemental proposed rule also moved these two provisions from Part 73, Appendix C, (in the proposed rule) to 10 CFR 50.54 of the final rule.

Both the proposed rule and the supplemental proposed rule received extensive stakeholder feedback. The consideration of stakeholder feedback and development of the final rule provisions resulted in several significant structural and content changes to the final rule provisions, which are briefly discussed below.

SIGNIFICANT CHANGES FROM THE PROPOSED TO FINAL RULE:

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

1. Separation of the Enhanced Weapons and Firearms Background Check Requirements. As discussed above, Section 161A of the AEA permits the NRC to authorize the use of certain enhanced weapons in the protective strategies of specific designated licensees once guidelines are developed by the NRC and approved by the Attorney General (from

Section 653 of EPAct 2005). In anticipation of the completion of those guidelines, the proposed rule contained several provisions that would have described the requirements for the use of enhanced weapons and for firearms background checks for certain security personnel (i.e., proposed § 73.18 and § 73.19). Since the guidelines have not yet received the approval of the Attorney General, the NRC staff has proposed in SECY-08-0055 (April 17, 2008) to separate that portion of the proposed rule to be continued as a separate rulemaking. As a result, this draft final rule does not contain any provisions related to the implementation of Section 161A.

2. Cyber Security Requirements. Another recommended change to this final rulemaking is the relocation of proposed cyber security requirements. Cyber security requirements had been located in the proposed rule in Paragraph 73.55(m). The staff recommends that these requirements now be placed into a new separate section within Part 73 (§ 73.54). The staff believes that these requirements are better suited for a stand-alone section to enable the cyber security requirements to be made applicable to other types of facilities and applications through future rulemakings. For licensing purposes, the cyber security plans would be dealt with consistent with the treatment of other security plans, generally in §§ 50.34, 50.54, 52.79, and 52.80, as applicable. For current reactor licensees, the staff recommends that the rule require the submission of a cyber security plan to the NRC for review and approval by way of a license amendment within 180 days of the effective date of the rule. For reactor applicants with an application currently before the NRC, they would be required to amend their applications to address the requirements of Section 73.54.

3. Performance Evaluation Program Requirements. The staff recommends that these requirements be moved in their entirety from Part 73, Appendix C, to Part 73, Appendix B, because these requirements describe the development and implementation of a program for training the security force in the response to contingency events.

4. Mitigative Strategies and Response Procedures for Potential or Actual Aircraft Attacks. In accordance with the supplemental proposed rule discussed earlier, the staff recommends that the mitigative measures and potential aircraft attack notification requirements that were initially located in proposed Part 73, Appendix C, now be located in Paragraph 50.54(hh) as a condition of an operating license. The staff made this change 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 and that clarification was needed. The staff clarified the language and added additional language to the proposed rule regarding licensee response to potential aircraft attacks.

5. Section 73.71 and Appendix G to Part 73. The proposed rule contained revisions to § 73.71 and Part 73, Appendix G. The NRC staff intended to recommend few changes to these regulations based on public comments. However, the staff recommends that these provisions are not contained in this final rule but that they are instead addressed as part of the enhanced weapons and firearms background checks rulemaking because conforming changes must be made to reporting requirements for licensees with regard to enhanced weapons.

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

licensees to revise, and submit for NRC review and approval, their physical security plan, safeguards contingency plan, and training and qualification plans to incorporate the new rule requirements. The staff recommends that the final rule no longer require these security plan submittals (with the notable exception of a cyber security plan discussed above) and instead permit current licensees to make changes in accordance with the criteria of §§ 50.54(p) or 50.90, as applicable. The NRC staff judged this approach to be acceptable because the great majority of the requirements in this final rule are substantially similar to the requirements that had been imposed by the orders and because all current licensees have security plans that addressed those requirements which were reviewed and approved by the NRC in 2004. In addition, many of the additional requirements in the final power reactor security rule are already current practices that were implemented in the site-specific plans. For these new rule requirements, the NRC staff is confident that most of these changes are security plan enhancements that could be incorporated into security plans consistent with the change process described in § 50.54(p). For the requirements that go beyond current practices, the staff does not expect that the changes required by this rule would result in a decrease of effectiveness in a licensee's security plan. If, in a licensee's judgment, a particular security plan change would reduce the effectiveness of the plan, then the proposed plan revision would be required to be submitted to the NRC for review and approval as a license amendment in accordance with § 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 would be required by this rule to amend their applications to the extent necessary to address the requirements of the new rule.

7. 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.

8. 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.

9. EPAct 2005 Provisions. The proposed rule contained a number of proposed requirements that were designed to address security-related provisions of the EPAct 2005. As noted above, the staff recommended that the EPAct 2005 Section-653 provisions for enhanced weapons and firearms background check requirements be moved to a separate rulemaking. Therefore, the only other provisions of the EPAct 2005 that the NRC had considered during this rulemaking were in Section 651, which concerns matters related to the triennial NRC-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 EPAct 2005 requires the NRC to be directly responsible for implementation of those requirements, the staff does not believe that any of these provisions need to be specifically reflected in the NRC's regulations.

FINAL RULE REQUIREMENTS:

This final rulemaking would amend the security requirements for power reactors and would include revisions to the following existing sections and appendices in 10 CFR Part 73:

- 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, General criteria for security personnel.
- 10 CFR Part 73, Appendix C, Licensee safeguards contingency plans.

The final rule would 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.

This rulemaking, if approved by the Commission, would contain a number of significant new requirements discussed below.

1. Safety/Security Interface Requirements. These requirements would be located in new Section 73.58. The safety/security requirements explicitly require licensee management to consider potential adverse interactions between security activities and other plant activities and 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.

2. Mixed-Oxide (MOX) Fuel Requirements. The staff recommends that these requirements be codified as new Paragraph 73.55(l) for reactor licensees who propose to use MOX fuel in concentrations of 20 percent or less. These new requirements provide enhancements to the normal radiological sabotage-based physical security requirements for the protection of the MOX fuel from theft or diversion. These requirements reflect the NRC staff's view that 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 MOX fuel

assemblies. The MOX fuel security requirements in this rule are consistent with the approach previously approved by the Commission and implemented at the Catawba Nuclear Station through the MOX lead test assembly effort in 2004-2005.

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

4. Mitigative Strategies and Response Procedures for Potential or Actual Aircraft Attacks. The staff recommends that these requirements be set forth in new § 50.54(hh). Section 50.54(hh)(1) would establish the necessary regulatory framework 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. The staff also recommends that § 50.54(hh)(2) require 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, order; specifically, the "B.5.a" and the "B.5.b" provisions.

5. Access Authorization Enhancements. The staff is recommending substantial revisions to existing § 73.56. The revisions would incorporate lessons-learned from the Commission's implementation of the January 7, 2003, order requirements and would improve integration of the access authorization requirements and security program requirements. The recommended final rule includes an increase in rigor for many elements of existing access authorization program requirements. In addition, the final rule requirements would include access authorization measures for individuals who could employ electronic means to adversely impact facility safety, security, or emergency preparedness; enhancements to the psychological assessment requirements; use of information sharing systems between reactor licensees; expanded behavioral observation requirements; reinvestigations of criminal and credit history records for all individuals with unescorted access; and 5-year psychological reassessments for individuals with certain critical job functions.

6. Training and Qualification Enhancements. These recommended requirements are set forth in the revised Part 73, Appendix B, and would include modifications to the training and qualification requirements based on insights from implementation of the security

orders, NRC reviews of site security plans, implementation of the enhanced baseline inspection program, and insights gained from evaluation of licensee force-on-force exercises. These new requirements would include additional physical fitness standards for unarmed security personnel to assure that personnel performing these functions meet minimum physical requirements commensurate with their duties. The new requirements also include a minimum age requirement of 18 years for unarmed security officers, increased minimum qualification scores for testing required by the training and qualification plan, enhanced qualification requirements for security trainers as well as drill and exercise controllers, personnel responsible for assessing psychological qualifications, armor certification requirements, and program requirements for on-the-job training.

7. Physical Security Enhancements. The staff recommends that the final rule impose new physical security measures in the revised §73.55 that have been identified by the staff during implementation of the security orders, reviews of site security plans, implementation of the enhanced baseline inspection program, and evaluations of licensee force-on-force exercises. Significant new requirements in §73.55 would include a requirement that the central alarm station (CAS) and secondary alarm station (SAS) have functionally equivalent capabilities such that no single act of radiological sabotage could disable the key functions of both CAS and SAS. Other significant recommended changes include requirements for new reactor licensees to locate the SAS within the 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 would also include requiring uninterruptible backup power supplies for detection and assessment equipment, real-time play-back video image equipment, and protection from waterborne vehicles.

PETITIONS FOR RULEMAKING:

Three petitions were considered during the development of the final rule requirements consistent with previous petition resolution and closure process for these petitions.

1. PRM-50-80. This PRM was submitted by the Union of Concerned Scientists (UCS) and the San Luis Obispo Mothers for Peace and was originally docketed and noticed for comment on June 16, 2003 (68 FR 35568). The petition requested that the NRC take two actions, the second of which was resolved as part of the final DBT rulemaking on March 19, 2007 (72 FR 12705). The first requested action 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 NRC approval. It was consolidated for consideration with the power reactor security rulemaking on November 17, 2005 (70 FR 69690). Proposed language addressing the issues raised in the petition was published as proposed Section 73.58, "Safety/security interface requirements for nuclear power reactors." This section remains in the final rule.

2. PRM-73-11. This PRM was submitted by Scott Portzline, Three Mile Island Alert, and was noticed for public comment on November 2, 2001 (66 FR 55603). In short, 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. As noted in a *Federal Register* Notice published December 27, 2006 (72 FR 481), the NRC consolidated PRM-73-11 and the public comments filed on the petition for consideration in this rulemaking. As noted in the draft final rule, the staff does not recommend incorporating the petitioner's suggestion into Part 73. The NRC staff concluded that establishing a prescriptive requirement to post armed security personnel in the OCA is not necessary. Instead, the final physical security requirements in § 73.55(k) would allow 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.

3. PRM-73-13. This PRM was submitted by the Union of Concerned Scientists and was noticed for public comment on April 9, 2007 (72 FR 17440). In summary, the petitioner requested several changes to the Commission's regulations related to unescorted and escorted access including requiring licensees to deny escorted or unescorted access to certain individuals and to require armed escorts for individuals for whom licensees are unable to acquire sufficient background information. The NRC determined that the issues raised in PRM-73-13 were appropriate for consideration in this rulemaking and consolidated the petition. For the reasons set forth in the attached *Federal Register* Notice, the staff does not recommend adoption of either proposal in the final rule.

RESOURCES:

Resources to complete the rulemaking (excluding inspection) are in the budget. Estimates follow:
FY 2009 NRR 0.6 FTE and $50K, NSIR 1.7 FTE
FY 2010 NSIR 0.5 FTE and $100K

NRR has requested 0.6 FTE and $50K for FY 2009 and NSIR has requested 1.7 FTE in their FY 2009 budget to Congress. For FY 2010, NSIR is requesting 0.5 FTE and $100K through the FY 2010 Planning, Budgeting, and Performance Management Process.

COMMITMENTS:

Fourteen draft regulatory guides have been developed or revised to support this rulemaking. The draft guides are prioritized into two groups. The first group of ten draft guides is directly tied to the new rule. They are drafted and have been distributed for public comment where appropriate or to limited-authorized interested persons where necessary to protect Safeguards Information. The staff plans to finalize the first group of guidance by February 2009. The second group of four draft guides must be revised and/or updated. The staff plans to finalize these guides by March 2009.

RECOMMENDATIONS:

That the Commission:

1. Approve for publication in the *Federal Register* the enclosed final rule (Enclosure 1).

2. To satisfy the requirement of the Regulatory Flexibility Act, 5 U.S.C. 605 (b), certify that this rule, if promulgated, will not have significant impact on a substantial number of small entities. This certification is included in the enclosed *Federal Register* Notice.

3. Notes:

   a. The Chief Counsel for Advocacy of the Small Business Administration will be informed of the certification and the reasons for it, as required by the Regulatory Flexibility Act, 5 U.S.C. 605(b).

   b. That a final Regulatory Analysis has been prepared for this rulemaking (Enclosure 2).

   c. The staff has determined that this action is not a "major rule" as defined in the Congressional Review Act of 1996 [5 U.S.C 804(2)] and has confirmed this determination with the Office of Management and Budget (OMB). The appropriate Congressional and Government Accountability Office contacts will be informed. The final rule imposes one-time costs that exceed $100 million. However, when those costs are annualized (i.e., spread out over an average 30-year lifetime of impacted facilities), the costs (as an annual impact on the economy) are much less than $100 million.

   d. The appropriate Congressional committees will be informed.

   e. A press release will be issued by the Office of Public Affairs when the final rulemaking is filed with the Office of the *Federal Register*.

   f. The final rule contains amended information collection requirements subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501, et seq.) that must be submitted to the OMB for its review and approval before publication of the final rule in the *Federal Register*.

COORDINATION:

The Office of the General Counsel has no legal objection to this final rulemaking. The Office of the Chief Financial Officer has reviewed this Commission paper for resource implications and has no objections. An information copy of this final rule was provided to the Committee to Review Generic Requirements. An information and status briefing was provided to the Advisory Committee on Reactor Safeguards (ACRS) on June 4, 2008. The ACRS review of the portions of this rulemaking within the committee's scope (i.e., §§ 50.54(hh), 73.58, and 73.54) was deferred until July 9, 2008, to expedite delivery of this final rule. The ACRS will provide its views and conclusions directly to the Commission.

/RA/

R. W. Borchardt
Executive Director
for Operations

Enclosures:
1. *Federal Register* Notice
2. Regulatory Analysis
3. Comment Response Document
4. Environmental Assessment

Committee on Reactor Safeguards (ACRS) on June 4, 2008. The ACRS review of the portions of this rulemaking within the committee's scope (i.e., §§ 50.54(hh), 73.58, and 73.54) was deferred until July 9, 2008, to expedite delivery of this final rule. The ACRS will provide its views and conclusions directly to the Commission.

/RA/

R. W. Borchardt
Executive Director
for Operations

Enclosures:
1. *Federal Register* Notice
2. Regulatory Analysis
3. Comment Response Document
4. Environmental Assessment

ADAMS Accession No.: Pkg - ML081780209 *concurred via email **concurred via memo
WITS: 200600491/EDATS: SECY-2008-0348

OFFICE	DPR/NRR	Tech Editor*	CFO*	OE*	ADM **	NSIR
NAME	T.Reed	MLesar	JDyer (LBarnett for)	CCarpenter	MLesar	RZimmerman (WDean for)
DATE	06/30/2008	06/25/2008	06/26/2008	06/23/2008	06/20/2008	06/27/2008
OFFICE	OIS	OGC	NRO	NRR	EDO	
NAME	MJanney	BJones	MJohnson	ELeeds (BBoger for)	RBorchardt	
DATE	06/26/2008	06/27/2008	06/24/2008	06/27/2008	07/09/2008	

OFFICIAL RECORD COPY

Notes:

1) RES/FSME/NMSS concurrence – discussions were held with these offices and they agreed that their concurrence was not needed.
2) Copy of this package was sent to the Regions for feedback – concurrence was not requested.

[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.

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.

Section 73.54(b), Analysis of Digital Computer and Communication Systems and Networks. 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 Regulatory Analysis -appendices	X	X	ML081680069 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) Security organization.

(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 contingency 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.

Regulatory Analysis and Backfit Analysis

Final Rulemaking:
Power Reactor Security Requirements

U.S. Nuclear Regulatory Commission
Office of Nuclear Reactor Regulation
Office of Nuclear Security and Incident Response

Table of Contents

Executive Summary

The Nuclear Regulatory Commission (NRC) is amending the current security regulations and adding new security requirements pertaining to nuclear power reactors. The rulemaking: (1) makes generically applicable many of the security requirements imposed by Commission orders issued after the terrorist attacks of September 11, 2001, (2) adds several new requirements that resulted from insights gained while implementing the security orders, reviewing site security plans, and implementing the enhanced baseline inspection program and force-on-force exercises, (3) updates the regulatory framework in preparation for receiving license applications for new reactors, (4) imposes requirements to assess and manage site activities that can adversely affect safety and security, and (5) considered three petitions for rulemaking (PRM) as part of the effort to develop the security requirements. The safety and security requirements (in § 73.58) address, in part, PRM-50-80 that requested the establishment of regulations governing changes to facilities which could adversely affect the protection against radiological sabotage. The other two PRMs considered as part of this rulemaking were PRM-73-11 and PRM-73-13.

Several significant changes to this rulemaking occurred after the proposed rule stage. The final power reactor security rule does not contain the weapons provisions (§§ 73.18 and 73.19) and the reporting provisions (§ 73.71 and appendix G to part 73) that were included as part of the proposed rule. These provisions are being addressed in a separate rulemaking. Additionally, the cyber requirements that were in proposed § 73.55 were moved to a stand-alone section within part 73: § 73.54. Requirements stemming from section B.5 of the 2002 Interim Compensatory Measures (EA-02-026) order (regarding licensee procedures for responding to notifications of potential aircraft threats and for developing guidance and strategies to address the loss of large areas of the plant due to explosions or fires from a beyond-design basis event), that were contained in proposed appendix C to part 73, have been moved to 10 CFR 50.54(hh) and were republished as a supplemental proposed rule in April 10, 2008 (73 FR 19443). The proposed § 73.2 definitions (most of which applied to the proposed weapons provisions in §§ 73.18 and 73.19) that remain applicable are no longer in the final rule, and instead will be addressed in supporting guidance.

The analysis presented in this document examines the benefits and costs of the final security requirements relative to the baseline of existing security requirements, including current regulations and the relevant orders. The key findings of the analysis are as follows:

- Total Cost to Industry. The final rule will result in a total one-time cost to all nuclear power plant sites of approximately $115.71 million, followed by total annual costs on the order of $38.65 million. The total present value of these costs is estimated at $590.23 million (using a 7-percent discount rate) and $857.33 million (using a 3-percent discount rate) over the next 30 years.

- Average Cost per Site. The average nuclear power plant site, which may include multiple units, will incur a one-time cost of approximately $1.78 million followed by annual costs of approximately $594,600.

- Annual Impact to the Economy. The final rule will result in an annual impact to the economy of approximately $47.36 million (using a 7 percent discount rate, annualizing the one-time costs over 30 years, and adding these “annualized” one-time costs to the annual costs) or $44.38 (using a 3 percent discount rate). This final rule is therefore not a major rule as defined by the Congressional Review Act.

- Value of Benefits Not Reflected Above. With the exception of some of the direct monetary savings to industry, the cost figures shown above do not reflect the value of the benefits of the final rule. These benefits are evaluated qualitatively in Section 4.1. This regulatory analysis concluded the costs of the rule are justified in view of the qualitative benefits.

- Costs to NRC. The rule will result in a one-time cost to NRC of approximately $2.60 million. NRC is not expected to incur substantial annual costs as a result of the rule.

- Decision Rationale. Although the NRC did not quantify the benefits of this rule, the staff did qualitatively examine benefits and concluded that the rule will provide safety and security-related benefits. The sum total of the requirements in the final rule will provide additional assurance of licensees’ capabilities to protect power reactor sites against an assault as defined by the DBT of radiological sabotage. Specifically, the final rule will require that a single act of radiological sabotage cannot simultaneously disable the function of both CAS and SAS. The rule also requires certain electronic equipment used for alarms and communications to have uninterruptible backup power. The final rule will result in the deployment of certain technological advances in intrusion detection systems that are necessary during a safeguards contingency event. In recognition of advancing digital technology, the final rule will maintain the intent of the security orders by establishing the requirement for a cyber security program to protect any systems that, if compromised, could adversely impact safety, security or emergency preparedness. The final rule will increase licensees' security programs’ effectiveness through additional training and procedures such as safety/security interface, on-the-job training, and recurring criminal and credit history checks, and psychological assessments. The final rule access authorization amendments will improve the integration of the access authorization requirements, fitness-for-duty requirements, and security program requirements by increasing the rigor for some elements of the access authorization program, developing procedures to provide communication between a licensed psychologist or psychiatrist and other medical personnel, and adding requirements that subject additional individuals (such as those who have electronic access via computer systems or those who administer the access authorization program) to the access authorization requirements. NRC believes that these factors represent a substantial increase in safety and that the costs of the final rulemaking are justified based on these qualitative benefits.

The rule requirements will apply to new reactors, including Watts Bar Unit 2 (although it is important to note that Watts Bar Unit 2 is specifically required to meet the requirements applicable to current licensees) and any units that would be built under the new reactor applications that NRC has received to date. Because security program costs are largely a site-

based function, rather than a reactor-based function, the regulatory analysis and backfit analysis reflect costs associated with the co-located new reactors (currently that is Watts Bar Unit 2 and seven of the nine applications). For the new reactor applications that would place new reactors at sites that are not co-located (currently two applications) with operating reactors, this analysis estimates that one-time and annual impacts will be less than or equal to the corresponding impacts for operating reactors (i.e., because the development of security plans and systems for the new sites will not require that existing plans and systems be analyzed and reworked). However, the quantitative results do not reflect any additional incremental cost for the non-co-located reactors due to the uncertainty associated with when and if these facilities actually will be licensed and operated.

Abbreviations

AA	Access Authorization
DBT	Design Basis Threat
CAS	Central Alarm Station
CFR	Code of Federal Regulations
CRGR	Committee to Review Generic Requirements
DBT	Design-Basis Threat
ICM	Interim Compensatory Measure
NRC	Nuclear Regulatory Commission
OCA	Owner Controlled Area
PA	Protected Area
PRM	Petition for Rulemaking
SAS	Secondary Alarm Station
UCS	Union of Concerned Scientists

1. Introduction

This document presents a regulatory analysis of final revisions to the power reactor security requirements as set forth by the U.S. Nuclear Regulatory Commission (NRC) in Title 10, part 73, of the Code of Federal Regulations (10 CFR part 73). This introduction is divided into three sections. Section 1.1 states the problem and the reasons for the final rulemaking, Section 1.2 provides background information on the power reactor security rulemaking, and Section 1.3 discusses regulatory objectives related to adoption of the final revisions to the power reactor security rulemaking.

1.1 Statement of the Problem and Reasons for the Rulemaking

Following the terrorist attacks that occurred on September 11, 2001, the NRC conducted a thorough review of security to ensure that nuclear power plants and other licensed facilities continued to have effective security measures in place given the changing threat environment. Through a series of orders, the Commission specified a supplement to the Design Basis Threat (DBT), as well as requirements for specific training enhancements, access authorization enhancements, security officer work hours, and enhancements to defensive strategies, mitigative measures, and integrated response. Additionally, in generic communications, the Commission specified expectations for enhanced notifications to the NRC for certain security events or suspicious activities.

While those specific requirements are Safeguards Information (SGI), in general the changes resulted in enhancements 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 and military 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 checks.

The NRC, in implementing the security orders, reviewing the revised site security plans across the fleet of reactors, conducting the enhanced baseline inspection program, and evaluating force-on-force exercises, identified additional security measures that would provide added assurance of licensees' capability to protect against the DBT.

In addition, three petitions for rulemaking (PRMs) were addressed or considered as part of this rulemaking. PRM-50-80, submitted by David Lochbaum on behalf of the Union of Concerned Scientists (UCS) and San Luis Obispo Mothers for Peace, requested the establishment of regulations governing changes to facilities which could adversely affect their protection against radiological sabotage. This petition was partially granted on November 17, 2005 (70 FR 69690), and the new § 73.58 "Safety/security interface requirements for nuclear power reactors" contains requirements to address this aspect of the petition. PRM-73-11, submitted by Scott Portzline on behalf of Three Mile Island Alert, requested that the regulations governing physical

security be amended to require armed guards at the entrances to the owner controlled areas. This request was considered as part of the development of the final § 73.55 requirements. However, contrary to the request, the NRC is not requiring armed guards at the entrances of the owner controlled area as discussed in section II of the final rule Federal Register notice. Finally, PRM-73-13, submitted by David Lochbaum on behalf of UCS, requested that the requirements governing escort within, and access to, the protected area of the power reactor facility be amended to require armed escorts and to deny access to the protected area for individuals for which information becomes known that would prevent such an individual from gaining unescorted access. This PRM was considered as part of the effort to finalize both the § 73.56 and § 73.55 requirements. The NRC is not adopting either of the recommendations of the petition as discussed in section II of the final rule Federal Register notice.

1.2 Background

1.2.1 Current Regulations Governing Power Reactor Security (10 CFR Part 73)

NRC's regulatory requirements for the physical protection of plants and materials are contained in 10 CFR part 73. Part 73 distinguishes between requirements applicable to power reactors and to special nuclear material at fixed sites and in transit. Requirements for fixed sites vary depending on the type of site and the relevant DBT as described in § 73.1(a). The physical protection requirements for nuclear power reactors are contained in § 73.55 and focus on protecting against the DBT of radiological sabotage.

To protect against this DBT, the current requirements in § 73.55 that this rule will amend begin by establishing the following general objective (§ 73.55(a)):

> The licensee shall establish and maintain an onsite physical protection system and 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. The physical protection system shall be designed to protect against the design basis threat of radiological sabotage as stated in § 73.1(a).

In the current §§ 73.55(b)-(h) that this final rule will amend, the regulation establishes detailed requirements addressing the following aspects of licensees' physical protection systems:

- Physical security organizations,
- Physical barriers,
- Access requirements,
- Detection aids,

- Communications,
- Testing and maintenance procedures, and
- Response requirements.

Some of the provisions within the paragraphs identified above are particularly relevant to this analysis and are briefly described or summarized below.

Security Plans

Under 10 CFR 50.34(c), applicants for an operating license for a production or utilization facility are required to develop a security plan for NRC review and approval. 10 CFR 73.55(b), paragraphs (1)(i) and (3)(i) require licensees to maintain safeguards in accordance with their security plans and procedures. The security plan describes how the licensee or applicant will meet the requirements of part 73 (including the requirements for barriers, access requirements, systems, and equipment as required in §§ 73.55(b)-(h)).

Safeguards Contingency Plans

Under 10 CFR 50.34(d), applicants for an operating license for a production or utilization facility are required to develop a safeguards contingency plan in accordance with the criteria set forth in appendix C to 10 CFR part 73. The safeguards contingency plan must include plans for protecting against threats, thefts, and radiological sabotage. Under § 73.55(h)(1), licensees must maintain and implement their NRC-approved safeguards contingency plan. In accordance with 10 CFR part 73, appendix C, the goals of this plan are (1) to organize the response effort at the licensee level, (2) to provide predetermined, structured responses by licensees to safeguards contingencies, (3) to ensure the integration of the licensee response with the responses by other entities, and (4) to achieve a measurable performance in response capability.

Training and Qualification Plan

Under § 73.55(b)(4)(ii), licensees are required to establish, maintain, and implement an NRC-approved training and qualification plan outlining the processes by which security personnel will be selected, trained, equipped, tested, and qualified in accordance with appendix B to 10 CFR part 73.

1.2.2 Commission Orders

The Commission imposed four security orders on all operating power reactor licensees following September 11, 2001:

- EA-02-026, "Interim Compensatory Measures (ICM) Order," dated February 25, 2002, 67 FR 9792 (March 4, 2002);

- EA-02-261, "Access Authorization Order," dated January 7, 2003, 68 FR 1643 (January 13, 2003);
- EA-03-039, "Security Personnel Training and Qualification Requirements (Training) Order," dated April 29, 2003, 68 FR 24514 (May 7, 2003); and
- EA-03-086, “Revised Design Basis Threat Order,” dated April 29, 2003, 68 FR 24517 (May 7, 2003).

The specifics of the security changes contained in the security orders are controlled as SGI per § 73.21 but some of the general security enhancements are discussed briefly. The “ICM Order” required licenses to implement various security actions, such as: review and update the security and emergency plans to maximize compatibility, assess the adequacy of staffing plans at emergency response facilities, identify alternative facilities capable of supporting emergency response, conduct a review to ensure that responders are not assigned collateral duties that would prevent effective emergency response, and implement site-specific Emergency Action Levels (EALs) to provide an anticipatory response to a credible threat. The “Access Authorization Order” required licensees to enhance the access authorization (AA) program in § 73.56 by requiring more restrictive site access controls for personnel, including expanded, expedited, and more thorough employee background checks. The “Security Personnel Training and Qualification Requirements Order” required licensees to take measures to improve tactical and firearms proficiency and physical fitness of the security forces at nuclear power reactor facilities. Finally, the “Revised DBT Order” required all licensees to revise their physical security plans, safeguards contingency plans, and guard training and qualification plans required by 10 CFR §§ 50.34(c), 50.34(d), and 73.55(b)(4)(ii) to provide protection against this revised DBT.

Nuclear power plant licensees revised their security plans, training and qualification plans, and safeguards contingency plans in response to these orders. The NRC completed its review and approval of all of the revised security plans, training and qualification plans, and safeguards contingency plans on October 29, 2004.

1.3 Regulatory Objectives

The NRC’s objectives for the current rulemaking are to establish and update generically applicable security requirements similar to those previously imposed by the Commission orders issued after the terrorist attacks of September 11, 2001. Additionally, the rulemaking adds several new requirements, not derived directly from the Order requirements, requirements 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. The rulemaking also updates the regulatory framework in preparation for the licensing of new nuclear power plants. Finally, it resolves three petitions for rulemaking that were considered during the development of the final rule requirements.

2. Identification and Preliminary Analysis of Alternative Approaches

This section presents preliminary analysis of the alternatives that the staff considered to meet the regulatory goals identified in the previous section. (Section 4 presents a more detailed analysis of the final rule option.) The staff considered two alternatives for revising the power reactor security requirements as discussed below.

2.1 Option 1: No Action

Under Option 1, the no-action alternative, NRC would not amend the current regulations regarding power reactor security. Licensees would continue to comply with the Commission's security orders. This option would avoid certain costs that the rule would impose. However, taking no action would not address several "lessons-learned" identified during the time since the initial review and implementation of the orders. Additionally, taking no action would present a problem for the licensing of new reactors that did not receive the orders. The NRC's security regulations would be out of date, and not represent the minimum requirements the Commission deems necessary to ensure the adequate protection of public health and safety and the common defense and security. This would directly conflict with the Commission's licensing obligations set forth in Section 182 of the Atomic Energy Act of 1954, as amended (AEA).

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

Under Option 2, NRC would conduct a rulemaking to address changes in several sections of 10 CFR part 73 to enhance security operations at power reactors. These changes entail: (1) revising § 73.55, § 73.56, appendix B, appendix C, and (2) adding § 73.58 to introduce "safety/security interface" requirements and § 73.54 (formerly in § 73.55) to introduce cyber security requirements. 10 CFR part 50 would be revised to contain § 50.54(hh) (formerly in appendix C to part 73) which contains requirements regarding licensee procedures for responding to notifications of potential aircraft threats and for developing guidance and strategies to address the loss of large areas of the plant due to explosions or fires from a beyond-design basis event.

A comprehensive rulemaking would provide a means of addressing the identified issues and concerns with respect to part 73. Through a comprehensive revision, the NRC could (1) ensure that all power reactor licensees and applicants would be subject to uniform regulatory requirements in order to consistently implement measures to enhance security and safety at nuclear power plants; (2) revise current requirements to provide licensees and applicants with some implementation flexibility; (3) address adjustments and changes in security plans that licensees have adopted through the development of the revised licensee security plans; and (4) clarify the language of the existing rule. In addition, codification of these security requirements would enable the NRC to require appropriate security measures for new reactor applicants, permitting it to fulfill the NRC's statutory obligations under the AEA.

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

3. Evaluation of Benefits and Costs

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

3.1 Identification of Affected Attributes

This section identifies the factors within the public and private sectors that the regulatory alternatives (discussed in Section 2) are expected to affect. These factors are classified as "attributes" using the list of potential attributes provided by NRC in Chapter 5 of its *Regulatory Analysis Technical Evaluation Handbook*.[1] Affected attributes include the following:

- Safeguards and Security Considerations – The actions are intended to establish requirements that will provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public heath and safety.

- Public Health (Accident) – The action will reduce the risk that public health will be affected by radiological releases resulting from radiological sabotage.

- Occupational Health (Accident) – The action will reduce the risk that occupational health will be affected by radiological releases resulting from radiological sabotage.

- Industry Implementation – The action will require licensees to make facility modifications and to revise their Physical Security Plans, Safeguards Contingency Plans, and Training and Qualification Plans, among other implementation activities. Licensees will be required to submit cyber security plans for NRC review and approval.

- Industry Operation – The action will require licensees to conduct additional security activities beyond those currently required. For example, licensees will need to provide additional on-the-job training for security personnel. The action will also provide licensees with flexibility in eliminating or reducing certain activities. For example, vehicles operated inside a site protected area by an individual with unescorted access to the protected area will no longer need a security escort.

- NRC Implementation – Under the action, NRC will develop or revise guidance and inspection procedures and review changes to licensee security plans as a result of the new requirements.

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

- NRC Operation – The action will require the NRC Operations Center to answer calls from licensees when they discover an imminent or actual threat against the facility, and to answer calls regarding suspicious activity and tampering.

- Regulatory Efficiency – The action will result in enhanced regulatory efficiency through regulatory and compliance improvements, including changes associated with sites using mixed-oxide fuel assemblies.

- Off-Site Property – The action will reduce the risk that off-site property will be affected by radiological releases resulting from radiological sabotage.

- On-Site Property – The action will reduce the risk that on-site property will be affected by radiological releases resulting from radiological sabotage.

Attributes that are *not* expected to be affected under any of the rulemaking options include the following: occupational health (routine); public health (routine); environmental considerations; other government; general public; improvements in knowledge; and antitrust considerations.

3.2 Analytical Methodology

This section describes the process used to evaluate benefits and costs associated with the various regulatory options. The benefits of the rule include any desirable changes in affected attributes (e.g., monetary savings, improved safety resulting from new physical protection requirements) while the costs include any undesirable changes in affected attributes (e.g., monetary costs, increased exposures).

The analysis evaluates several attributes on a quantitative basis. (These include industry implementation, industry operation, NRC implementation, and NRC operation.) Quantitative analysis requires a baseline characterization, including factors such as the number of licensees affected, the nature of the activities currently being conducted, and the types of new or modified systems and procedures that licensees will implement, or will no longer implement, as a result of the rule. However, licensees may respond to the rule in different ways depending on their own site-specific characteristics, such as (1) the physical characteristics of their sites, (2) the current contents of their safeguards contingency plans, security plans, and training and qualification plans, (3) the organizational and managerial characteristics of their operations, and (4) their approaches toward meeting new performance-based criteria. It is beyond the scope of this analysis to characterize and analyze individually affected licensees, in large part because the information that would be needed consists of "Safeguards Information" that is protected under § 73.21.[2] Nevertheless, the analysis proceeds quantitatively for these attributes by making generalizing assumptions. Sections 3.2.1–3.2.4 describe the most significant analytical data and assumptions used in the quantitative analysis of these attributes. Additional details regarding the calculations used in the analysis are presented in the appendices to the analysis.

[2] Safeguards Information under 10 CFR 73.21 includes, for example, Security Plans, Safeguard Contingency Plans, physical protection system designs, security procedures, and information relating to safeguards inspections, audits, and evaluations.

The analysis relies primarily on a qualitative (rather than quantitative) evaluation of several of the affected attributes (safeguards and security considerations, public health, occupational health, offsite property, and onsite property) due to the difficulty in quantifying the impact of the current rulemaking.[3] These attributes will be affected by the regulatory options through the associated reduction in the risks of radiological sabotage damage to the reactor core and the spent fuel. Quantification of any of these attributes would require estimation of factors such as (1) the frequency of attempted radiological sabotage, (2) the frequency with which radiological sabotage attempts are (i.e., pre-rule) and will be (i.e., post-rule) successful, and (3) the impacts associated with successful radiological sabotage attempts.

3.2.1 Baseline for Analysis

This regulatory analysis measures the incremental impacts of the final rule relative to a "baseline," which reflects anticipated behavior in the event that the final regulation is not imposed. The baseline used in this analysis assumes full licensee compliance with existing NRC requirements, including current regulations and relevant orders. Section 4.1 presents the estimated incremental costs and savings of the final rule relative to this baseline.

3.2.2 Security Programs and Program Characteristics

The analysis models 65 sites comprising a total of 104 operating power reactors. It assumes that incremental costs and savings accrue to sites independent of the number of reactor facilities located at each site. It also assumes that the manner in which operating reactors comply with current security requirements is substantially similar (except as indicated in appendix A) and that all operating nuclear power reactors are in full compliance with current requirements imposed by NRC's regulations and Commission orders. As a result, the analysis applies the same average cost per activity to each site, even though in reality some sites will incur higher or lower costs. Each operating licensee is assumed to apply for and receive a single 20-year license extension. Based on the extended license expiration dates, the analysis calculates the average remaining operating life across all reactors as 30 years. Therefore, costs and savings are estimated for the 65 reactor sites over a 30 year period, with each year's costs or savings discounted back at a 7-percent and 3-percent discount rate, in accordance with NUREG/BR-0058, Rev. 4, "Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission." (See Section 4.1 for these results.)

The final rule also would apply to new reactors. Note that although Watts Bar Unit 2 is a "new" reactor, it differs from the other new reactor applications since it is a continuation of a part 50 construction permit and it is specifically required to meet current licensee requirements. NRC has (as of May 2008) received nine applications to build new nuclear power reactors. For the seven new applications that like Watts Bar Unit 2 would co-locate new reactors with currently operating reactors, this analysis assumes that there is no significant additional incremental cost or savings incurred because security program costs are largely a site-based function, rather

[3] The regulatory efficiency attribute also is evaluated qualitatively, by definition. See NRC's *Regulatory Analysis Technical Evaluation Handbook*, Section 5.5.14.

than a reactor-based function. For the two COL applications that would place new reactors at sites that are not co-located with operating reactors, this analysis estimates that one-time and annual impacts will be less than or equal to the corresponding impacts for operating reactors (i.e., because the development of security plans and systems for the new sites will not require that existing plans and systems be analyzed and reworked). Nevertheless, Section 4 does not reflect any additional incremental cost for the non-co-located reactors due to the uncertainty associated with when and if these facilities actually will be licensed and operated.

3.2.3 Data

Information on operating reactors and shutdown dates has been taken from NUREG-1350, Vol. 19, *NRC Information Digest, 2007-2008 Edition.* To the extent practical, quantitative information (e.g., costs and savings) and qualitative information (e.g., the nature and magnitude of safeguards and security impacts) on attributes affected by the rule has been obtained from, or developed in consultation with, NRC staff, commercial vendors, and available Nuclear Energy Institute data. NRC headquarters and regional staffs discussed their understanding of the potential differences between the new requirements and the current security measures in place at existing licensees and have incorporated available, non-safeguards, information into this regulatory analysis. The NRC sought insight from stakeholders on implementing costs and related issues via questions in the proposed rule *Federal Register* notice and integrated this information into the final rule regulatory analysis.

3.2.4 Additional Assumptions

The analysis assumes that any one-time implementation costs are incurred in calendar year 2010. Ongoing costs of operation are also assumed to begin in 2010, and are modeled on an annual cost basis. Where appropriate, the analysis calculates incremental costs and benefits for only a percentage of sites. In these cases, the results presented in Section 4 for the average site will reflect an appropriate proration of the applicable cost or benefit. The detailed incremental cost and savings calculations are presented in Appendices A and B.

4. Results

This section presents the analytical results which are organized into five separate sections:

- Section 4.1 presents findings on the overall benefits and costs of the final rule under the main analysis.
- Section 4.2 considers the findings relative to NRC's backfit rule.
- Section 4.3 considers the findings on a disaggregated basis.
- Section 4.4 addresses the applicability of a safety goal evaluation to the current rulemaking.
- Section 4.5 describes the information that is provide to the Committee to Review Generic Requirements (CRGR) for information only.

4.1 Benefits and Costs

This section summarizes the benefits and costs estimated for the regulatory options. To the extent that the affected attributes could be analyzed quantitatively, the net effect of each option has been calculated and is presented below. However, some values and impacts could be evaluated only on a qualitative basis.

The results of the benefit-cost analysis are summarized in Exhibits 4-1 and 4-2. Relative to the no-action alternative (Option 1), Option 2 would result in a net quantitative impact estimated between $592.84 million and $859.93 million (7-percent and 3-percent discount rate, respectively), with the majority of the costs associated with Option 2 being incurred by industry.

The analysis estimates that Option 2 will result in qualitative benefits in the following attributes: regulatory efficiency, safeguards and security, public health (accident), occupational health (accident), off-site property, and on-site property. Specifically, the benefits will include enhanced regulatory efficiency through regulatory and compliance improvements, including changes in industry's planning efforts and in NRC's review and inspection efforts. In addition, the rule will result in an increased level of assurance that nuclear power plant licensees can defend against the DBT. There also will be a reduced risk that public health, occupational health, off-site property, and on-site property will be affected by radiological releases resulting from attempted sabotage.

Exhibit 4-1

Summary of Benefits/Savings and Costs/Burdens

Net Monetary Savings (or Costs) - Total Present Value	Non-Monetary Benefits/Costs
Option 1: No Action $0	*Qualitative Benefits and Costs:* None.
Option 2: Action **Industry:** ($590 million) using a 7% discount rate ($857 million) using a 3% discount rate **NRC:** ($2.60 million) using a 7% discount rate ($2.60 million) using a 3% discount rate	*Qualitative Benefits:* Safeguards and Security: Increased level of assurance that nuclear power plants are safeguarded from attacks up to, and including the DBT for radiological sabotage. Regulatory Efficiency: Enhanced regulatory efficiency through regulatory and compliance improvements, including changes in industry's planning efforts and in NRC's review and inspection efforts. Public Health (Accident): Reduced risk that public health will be affected by radiological releases resulting from radiological sabotage. Occupational Health (Accident): Reduced risk that occupational health will be affected by radiological releases resulting from radiological sabotage. Off-Site Property: Reduced risk that off-site property will be affected by radiological releases resulting from radiological sabotage. On-Site Property: Reduced risk that on-site property will be affected by radiological releases resulting from radiological sabotage. *Qualitative Costs:* None.

Exhibit 4-2
Industry Savings and Costs by Section

Section	Average per Site		Total - All Sites			
	One-Time Saving (Cost)	Annual Saving (Cost)	One-Time Saving (Cost)	Annual Saving (Cost)	NPV (7 percent)	NPV (3 percent)
Section 73.54						
Cyber Security Plan	($19,200)	-	($1,248,000)	-	($1,248,000)	($1,248,000)
Cyber Security	($1,175,000)	($275,000)	($76,375,000)	($17,875,000)	($295,838,424)	($419,368,626)
Subtotal for Section 73.54	($1,194,200)	($275,000)	($77,623,000)	($17,875,000)	($297,086,424)	($420,616,626)
Section 73.55						
Update Plans and Procedures	($124,000)	-	($8,060,000)	-	($8,060,000)	($8,060,000)
Video Capture	($42,000)	-	($2,730,000)	-	($2,730,000)	($2,730,000)
Training for Escorts	($4,000)	-	($260,000)	-	($260,000)	($260,000)
Two-Way Radios for Escorts	($3,600)	-	($234,000)	-	($234,000)	($234,000)
Escort Communication	($30,000)	-	($1,950,000)	-	($1,950,000)	($1,950,000)
Uninterrupted Power	($75,000)	-	($4,875,000)	-	($4,875,000)	($4,875,000)
No Single Act	($57,000)	-	($3,705,000)	-	($3,705,000)	($3,705,000)
Target Sets	($59,000)	($3,894)	($3,835,000)	($253,110)	($6,942,602)	($8,691,790)
Heightened Security	($8,000)	-	($520,000)	-	($520,000)	($520,000)
Escort of Vehicles	-	$15,000	-	$975,000	$11,970,732	$18,708,743
Subtotal for Section 73.55	($402,600)	$11,106	($26,169,000)	$721,890	($17,305,870)	($12,317,047)
Section 73.56						
Records	-	($56,000)	-	($3,640,000)	($44,690,734)	($69,845,975)
Individuals Subject to Authorization Program	($9,000)	($4,500)	($585,000)	($292,500)	($4,176,220)	($6,197,623)
Increased Sharing of Medical Records	($8,400)	-	($546,000)	-	($546,000)	($546,000)
5-Year Update of Psychological Assessments	($18,038)	($3,158)	($1,172,438)	($205,238)	($3,692,277)	($5,110,628)

Section 73.56 (continued)						
Development of Psychological Test Thresholds	($3,000)	-	($195,000)	-	($195,000)	($195,000)
Administration of Psychological Assessments (Tests and Interviews)	-	($17,050)	-	($1,108,250)	($13,606,732)	($21,265,605)
Subtotal for Section 73.56	*($38,438)*	*($80,708)*	*($2,498,438)*	*($5,245,988)*	*($66,906,962)*	*($103,160,830)*
Section 73.58						
Safety/Security Interface	($116,500)	($40,000)	($7,572,500)	($2,600,000)	($39,494,453)	($57,462,482)
Subtotal for Section 73.58	*($116,500)*	*($40,000)*	*($7,572,500)*	*($2,600,000)*	*($39,494,453)*	*($57,462,482)*
Section 73, Appendix B						
Physical/Medical Examinations for Security Personnel	($10,000)	($2,500)	($650,000)	($162,500)	($2,645,122)	($3,768,124)
On-The-Job Training	($6,000)	($7,000)	($390,000)	($455,000)	($5,976,342)	($9,120,747)
Qualification of Security Instructors	($6,000)	($1,000)	($390,000)	($65,000)	($1,188,049)	($1,637,250)
Armorer Certification	($6,400)	($9,504)	($416,000)	($617,760)	($8,000,656)	($12,269,860)
Physical Requirements for Security Organization Personnel	-	($4,000)	-	($260,000)	($3,192,195)	($4,988,998)
Drill Exercise	-	($186,000)	-	($12,090,000)	($148,437,079)	($231,988,416)
Subtotal for Section 73, Appendix B	*($28,400)*	*($210,004)*	*($1,846,000)*	*($13,650,260)*	*($169,439,443)*	*($263,773,394)*
Section 73, Appendix C						
None.						
Subtotal for Appendix 73, Appendix C	-	-	-	-	-	-
Total	**($1,780,138)**	**($594,606)**	**($115,708,938)**	**($38,649,358)**	**($590,233,152)**	**($857,330,379)**

Results in 2008 dollars.

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

- The NRC issued orders after September 11, 2001, that required power reactor licensees to implement interim compensatory measures to enhance cyber security at their sites. These security measures required an assessment sufficient to provide protection against the cyber threats at the time of the orders. Subsequently, the NRC amended the final DBT requirements in § 73.1(a) to contain cyber attacks (72 FR 12705, dated March 19, 2007). As licensees implement digital upgrades for many systems at their plants, the potential for adverse consequences from cyber threats will be increased. The final rule requirements will maintain and clarify the intent of the security orders and put into place requirements that are to ensure compliance with the revised DBT requirements, by establishing the requirement for a cyber security program to protect systems that, if compromised, can adversely impact safety, security or emergency preparedness.

- The final rule requires licensees to update their physical security, training and qualification, and safeguards contingency plans within 180 days of the effective date of the final rule. Licensees must revise the plans required by § 73.55(c) of the final rule, along with corresponding revisions to all relevant procedures. The new requirement ensures that licensees maintain up-to-date plans and procedures so that they are able to take appropriate actions in preparation for and response to a security-related incident.

- Current requirements at 10 CFR 73.55(h)6) address the use of closed circuit television systems for monitoring of the protected area perimeter, but do not explicitly require them. Nonetheless, the NRC is aware that all licensees have adopted the use of video surveillance in their site security plans, and many licensees have adopted advanced video surveillance technology to provide real-time and play-back/recorded video images to help security officials determine the cause of an alarm annunciation. The final rule, in paragraph 73.55(e), requires the monitoring of isolation zones with assessment equipment that can provide real-time and play-back/recorded video images. Advanced video technology will provide greater assurance that a licensee can assess the cause of an alarm annunciation and initiate a timely response capable of defending the facility against hostile acts up to and including the design basis threat.

- The final rule, paragraph 73.55(g)(8), will ensure that escorts are trained and knowledgeable of their duties while accompanying visitors. This requirement will reduce the risk of a security incident initiated by a visitor because escorts will be better informed regarding visitor's authorized activities.

- The final rule, paragraph 73.55(g)(8)(ii), requires that licensees ensure that individuals assigned to visitor escort duties are provided a means of timely communication with security personnel in a manner that ensures the ability to summon assistance when needed. The new requirement improves security at sites by ensuring that escorts have the ability to call for assistance before that capability can be removed as the result of a security-related incident.

- The final rule, paragraph 73.55(g)(8)(iii), states that each individual assigned to vehicle escort duties must be capable of maintaining continuous communication with security personnel to ensure the ability to summon assistance when needed. This new requirement ensures that escorts have the ability to maintain a direct line of communication with security personnel (e.g., by radio).

- Current regulatory requirements at 10 CFR 73.55(e) and (f) require that both CAS and SAS have equivalent alarm annunciation and communication capabilities, but do not explicitly require equivalent assessment, monitoring, observation, and surveillance capabilities. Further, the current requirement of § 73.55(e)(1) states "All alarms required pursuant to this part must annunciate in a continuously manned central alarm station located within the protected area and in at least one other continuously manned station not necessarily onsite, so that a single act cannot remove the capability of calling for assistance or otherwise responding to an alarm." The Commission orders added enhanced detection and assessment capabilities, but did not require equivalent capabilities for both CAS and SAS. The security plans approved by the Commission on October 29, 2004, varied, due to the performance-based nature of the requirements, with respect to how the individual licensees implemented these requirements, but all sites were required to provide CAS and SAS with functionally equivalent capabilities to support the implementation of the site protective strategy.

  Section 73.55(i)(4)(iii) of the final rule states that applicants for an operating license under the provisions of part 50, or holders of a combined license under the provisions of part 52, shall construct, locate, protect, and equip both the central and secondary alarm stations to the standards for the central alarm station in § 73.55, and that 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. However, this requirement does not apply to current licensees or new reactors that use a design certified before the final rule takes effect. For new reactors covered by COL applications that already have been submitted to the NRC, therefore, the NRC staff believes this requirement will not be applicable.

- Paragraph 73.55(i)(4)(i) of the final rule requires protecting the alarm stations such that a single act does not disable the key functions will provide an enhanced level of assurance that a licensee can maintain detection, assessment and communications capabilities required to protect the facility against the design basis threat of radiological sabotage.

- Current regulatory requirements at 10 CFR 73.55(e)(1) require back-up power for alarm annunciation and non-portable communication equipment, but do not require uninterruptible back-up power. Although not specifically required, many licensees have installed uninterruptible power supplies to their security systems for added reliability. Uninterruptible back-up power for intrusion assessment and detection equipment at the protected area perimeter, as required now by paragraph 73.55(i)(2)(vii), will provide an enhanced level of assurance that a licensee can maintain capabilities required to defend

the facility against the design basis threat. This new requirement will reduce the risk of losing detection and assessment during a loss of the normal power supply.

- The development of target sets is not a current regulatory requirement. Although the orders did require licensees to maintain target sets, the final rule contains additional target set requirements. The final rule, paragraph 73.55(f), requires licensees to document and maintain the process used to develop and identify target sets, identify and document target set equipment or elements including equipment that is not contained within a protected or vital area, and update target set documentation as needed. Licensees benefit from the new target set requirements because the identification and protection of target sets is a critical component for the development and implementation of the licensee protective strategy.

- Paragraph 73.55(k)(1)) of the final rule requires licensees to establish, maintain and implement a threat warning system which identifies protective measures and actions to be taken to increase licensee preparedness against a heightened security threat. The primary benefit of the heightened security requirement is that licensees will be better prepared to respond to security-related incidents, thus increasing public health and safety.

- Vehicles operated inside a protected area (PA) by individuals with unescorted PA or vital area access no longer need a security escort, as was required by paragraph 73.55(d)(4). Under the final rule, paragraph 73.55(g)(3), only vehicles operated by individuals without unescorted access will need to be escorted, and only vehicles transporting hazardous materials need be escorted by an armed member of the security organization. Currently all vehicles inside the PA must be escorted by a member of the security organization, producing an unnecessary burden on the physical protection of a facility. This change is made possible by the improvement of the unescorted access authorization programs in § 73.56.

- The final rule, paragraph 73.56(b)(1)(ii), will require licensee access authorization programs to cover individuals whose job duties and responsibilities permit them to access or use digital computer systems that may affect licensees' operational safety and security systems, and emergency response capabilities. Historically, digital computer systems have played a limited role in the operation of nuclear power plants. However, the role of computer systems at nuclear power plants is increasing as licensees take advantage of digital technology to maximize plant productivity. In general, licensees currently exclude from their access authorization programs individuals who may electronically access equipment located in the protected areas of nuclear power, if their duties and responsibilities do not require physical unescorted access to the equipment located within protected or vital areas. However, because these individuals may manage and maintain the networks that connect to equipment located within protected or vital areas, and are responsible for permitting authorized and/or trusted personnel to gain electronic access to equipment and systems, they are often granted greater electronic privileges than the trusted and authorized personnel. With advancements in electronic technology and telecommunications, differences in the potential adverse

impacts of a saboteur's actions through physical access and electronic access are lessening. Thus, the final rule will require those individuals who have authority to access equipment electronically that, if compromised can adversely impact operational safety, security or emergency preparedness of the nuclear power plants, to be determined to be trustworthy and reliable.

- The final regulatory requirements at paragraph 73.56(e) specify that licensees, applicants, and contractors or vendors must develop procedures regarding communications between the licensed psychologist/psychiatrist and other medical personnel. The new requirement enables the licensed psychologist/psychiatrist to report any information, including a medical condition, that could adversely impact the fitness-for-duty, trustworthiness, or reliability of those individuals who have been granted unescorted access authorization status.

- The final rule, paragraph 73.56(e), requires a licensed psychiatrist or psychologist to administer the psychological assessment and it requires the licensed medical professional to develop thresholds for the psychological test. The predetermined thresholds will be applied in interpreting the results of the test to determine whether an individual must be interviewed by a licensed psychiatrist or psychologist. Additionally, paragraph 73.56(i)(1)(v)(B) of the final rule requires licensees to update psychological assessments every five years for those individuals who perform duties that are critical to the safety and security of the nuclear power plant. The new requirement not only provides greater consistency and accuracy of the psychological test, but also provides increased assurance that individuals who perform duties that are critical to the safety and security of the nuclear power plant are able to carry out their specific job functions effectively.

- Paragraph 73.56(o) of the final rule requires licensees to document and retain records relating to an individual's unescorted access authorization status and written agreement of services. The new requirement states that licensees must maintain these records for at least five years after an individual's unescorted access authorization has been removed. The requirement to retain all documentation and records for five years ensures that those individuals involved in legal proceedings related their termination of unescorted access have access to their records during the entire course of the legal proceedings.

- Section 73.58 of the final rule requires licensees to assess and manage potential adverse effects on safety and security when implementing changes to plant configurations, facility conditions or security. Licensees are required to review and update existing procedures to reference the safety/security interface requirements, as well as revise and update the corresponding guidance documents. The final safety/security interface requirements will reduce the risk of adverse safety/security interactions and enhance the communication among nuclear power plant staff.

- The NRC is aware that some licensees permit unarmed security personnel to perform duties similar to armed security personnel, including detection, assessment, vehicle and

personnel escort, and vital area controls. The current requirements for unarmed members of the security organization at 10 CFR part 73, appendix B, paragraph I.B.1.a. state in part that these individuals shall have no physical weaknesses or abnormalities that would affect their performance of assigned duties. However, the current rule does not require unarmed personnel to pass a physical examination to verify that they meet standards for vision, hearing, or some portions of psychological qualifications. Appendix B, VI.B.2(a)(2) of the final rule includes a requirement to assure that unarmed security personnel are physically capable of performing their assigned duties. Additionally, appendix B, paragraph I.A.2. of the current rule specifies a minimum age of 21 years for armed security personnel, but does not specify a minimum age requirement for unarmed security personnel. Appendix B, paragraph VI.B.1(a)(2) of the final rule requires that unarmed members attain the age of 18 years prior to assignment. These additional requirements will assure that personnel performing security functions whether, armed or unarmed, meet appropriate age, vision, hearing and psychological requirements commensurate with their assigned security duties.

- The current rule states at appendix B, paragraph II.D., in part, that each individual is assigned security duties shall, prior to assignment, be trained to perform these tasks and duties, and must demonstrate the required knowledge, skill and ability in accordance with specific standards of each task. Appendix B, paragraph VI.C.2. of the final rule now requires licensees to develop on-the-job training plans and procedures. The on-the-job training program will provide licensees the ability to assess an individual's knowledge, skill, and ability to effectively carry out assigned duties, in a supervised manner within the actual work environment, before assignment to an unsupervised position.

- The current rule and the security orders do not specifically address the qualification or certification of instructors, or other personnel that have assigned duties and responsibilities for implementation of training and qualification programs at power reactor licensees. Appendix B, paragraph IV.E of the final rule includes requirements that personnel who have assigned duties and responsibilities for implementation of training and qualification programs be qualified and/or certified to make determinations of the suitability of security personnel. These requirements will result in more effective training, which subsequently results in a more effective security force.

- Appendix B, paragraph VI.G.3.(a) of the final rule requires licensees to develop a firearms maintenance and accountability program that includes armorer certification. To implement this rule requirement, armorers will need to get training and certification on the weapons used at their facility (this regulatory analysis assumes that each armorer will receive one week of training per weapon every three years). This requirement will increase safety by ensuring that weapons and ammunition are properly maintained, function as designed, and are properly stored and accounted for. Additionally, the armorer certification requirement will provide licensees with the assurance that security personnel have functional equipment to assume their security duties upon assignment.

- The current rule and the security orders do not specifically address the qualification of personnel who have assigned duties and responsibilities for implementing security-

related training and qualification drills and exercises at power reactor licensees. Appendix B, paragraph VI.C.3.(l)(4) of the final rule will include requirements for personnel that function as drill and exercise controllers to ensure these persons are trained and qualified to execute their assigned duties. Drills and exercises are key elements to assuring the preparedness of the security force. Performing drills with qualified personnel provides added assurance that the drills and exercises will provide meaningful results and improve a licensee's ability to implement the protective strategy as described in the site security plans effectively.

4.2 Backfit Analysis

This section presents the NRC's evaluation of changes in the rule in accordance with the Backfit Rule, § 50.109.

The backfit analysis examines the aggregation of the subset of power reactor security requirements that constitute backfitting as defined in 10 CFR 50.109(a)(1). These provisions are identified later in this section. The backfit analysis examines the impacts of the rule relative to the baseline used in the regulatory analysis, which consists of existing requirements stated in 10 CFR part 73 as well as requirements in the recently issued orders. The analysis excludes individual requirements that are not subject to the Backfit Rule or that are not backfitting by definition, which includes requirements that fall into one or more of the following categories:

- Administrative matters. Revisions that make minor administrative changes, such as correction of typographic errors, correction of inconsistencies, relocating requirements from one section to another, and combining existing requirements into a single section.

- Information collection and reporting requirements. Revisions that either amend existing information collection and reporting requirements or impose new information and collection and reporting requirements, which are not considered to be backfits, as set forth in the Committee to Review Generic Requirements (CRGR) charter.

- Clarifications. Revisions that clarify current requirements to assure consistent understanding and implementation of the NRC's original intent for these requirements. These revisions remove the ambiguities that produced regulatory uncertainty without changing the underlying requirements stated in these sections.

- Permissive relaxations/Voluntary alternatives. Revisions that permit, but do not require, relaxations or alternatives to current requirements (i.e., licensees are free to either comply with current requirements or adopt the relaxed requirements/voluntary alternative as a binding requirement).

- Requirements that are similar to the provisions required by the recent Commission orders (Interim Compensatory Measures (ICM), February 25, 2002;

> Access Authorization, January 7, 2003; Revised Design Basis Threat, April 29, 2003, and; Security Personnel Training and Qualification Requirements (Training), April 29, 2003) are not backfitting as defined by 10 CFR 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. Nonetheless, 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 and are in accord with the common defense and security. Therefore, no backfit analysis has been prepared with respect to these requirements

The NRC then evaluated the aggregated set of requirements constituting backfitting in accordance with § 50.109, and not subject to one of the exceptions stated in paragraph 50.109(a)(4), 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. In performing this analysis, the NRC considered the quantitative and qualitative costs and benefits of the rule, as discussed below.

Security Regulatory Requirements that Constitute Backfitting

- The cyber security plan must be approved by the Commission and must establish procedures to comply with cyber security programmatic requirements, such as training and hardware modifications, in accordance with § 73.54.

- Security plans and procedures (excluding the cyber security plan, which is analyzed separately in § 73.54) must be revised to address certain requirements in the final rule, though these plans do not have to be submitted to the NRC for prior approval.

- Assessment capabilities must include specialized video surveillance equipment.

- All personnel assigned escort duty must be properly trained and meet other minimum standards, such as access authorization, communication abilities, knowledge of authorized activities, and description of escort-visitor ratios.

- All individuals assigned to escort personnel must be provided with a means of timely and continuous communication.

- Uninterruptible power supplies to maintain alarm and assessment capabilities are required.

- No single act can cause the loss of key functions in both alarm stations.

- Target set equipment documentation and maintenance must be developed in accordance with the requirement set forth in § 73.55.

- Licensees must establish, maintain, and implement a threat warning system.

- Licensees must implement enhanced access authorization requirements.

- Licensees must develop new procedures to increase communication between the licensed psychologist or psychiatrist and the licensee.

- A licensed psychologist or psychiatrist must administer the psychological assessment, using pre-determined thresholds developed by a medical professional to assess the mental state of the individual receiving the test.

- Licensees must revise existing “change control” procedures to address safety/security interface requirements.

- Licensees must test the vision, hearing, and medical condition of unarmed members of the security organization assigned to "unsupervised" duties involving detection, assessment, and response.

- Licensees must provide additional on-the-job training to security personnel including developing on-the-job training plans and procedures.

- Licensees must ensure that security instructors receive specified training to qualify them to perform their duties.

- Licensees must implement a firearms maintenance and accountability program that includes armorer certification.

- Unarmed security personnel must, on an annual basis, meet physical requirements commensurate with their duties.

- Licensees must conduct drills and exercises in accordance with NRC-approved security plans.

Collectively, the requirements in the rule that qualify as backfitting will result in an estimated net cost of approximately $590.23 million to industry over the next 30 years (present value), assuming a 7-percent discount rate, or approximately $857.33 million assuming a 3-percent discount rate.

For the average site, these backfits will result in an initial one-time cost of approximately $1.78 million, followed by annual costs of about $594,600 per year. For industry as a whole, NRC estimates that the backfits will result in approximately $115.71 million in one-time costs, and about $38.65 million in annual costs.

The final rule will result in an annual impact to the economy of approximately $47.36 million (using a 7 percent discount rate, annualizing the one-time costs over 30 years, and adding these “annualized” one-time costs to the annual costs) or $44.38 (using a 3 percent discount rate). This final rule is therefore not a major rule as defined by the Congressional Review Act.

The NRC evaluated the safety benefits afforded by the backfitting resulting from the final power reactor security rule revisions, as documented in Section 4.1 of the regulatory analysis, in qualitative terms. (See Section 3.2 of this document for a discussion of the issues that will be involved in quantifying the benefits of the rule.) NRC also qualitatively determined whether the costs of the backfitting required by this rule will be justified in light of the safety benefits. By contrast, the NRC evaluated backfitting costs and cost reductions in quantitative terms, as documented in appendix A of this regulatory analysis.

In performing this analysis, the NRC considered the nine factors in § 50.109, as follows:

(1) Statement of the specific objectives that the backfit is designed to achieve;

The rulemaking constitutes an integrated regulatory initiative directed at the singular regulatory matter of security requirements at nuclear facilities. The goals of the final rule will be as follows:

- Make generically applicable security requirements similar to those imposed by Commission orders issued after the terrorist attacks of September 11, 2001, based upon experience and insights gained by the Commission during implementation.

- Add several new requirements that resulted from insights from implementation of the security orders, review of site security plans, and implementation of the enhanced baseline inspection program and force-on-force exercises.

- Update the regulatory framework for the licensing of new reactors.

- Impose requirements to assess and manage site activities that can adversely affect safety and security.

(2) General description of the activity that will be required by the licensee or applicant in order to complete the backfit;

In general terms, the final rule will require that all current and future power reactor licensees consistently implement new and existing security measures. These new measures include revisions to existing "change control" procedures to address safety/security interface requirements to avoid adverse safety-security interactions. The backfits include several requirements targeted at enhancing intrusion detection and assessment system technologies in the CAS and SAS. These enhancements include uninterruptible power for detection and assessment equipment. The backfits required in appendix B address physical qualifications and training for security personnel. The final rule extends armed security personnel requirements for vision, hearing, medical, and physical qualifications to unarmed security personnel, commensurate with their duties. In terms of training, the final rule requires on-the-job training for armed and unarmed members of the security organization, qualification of training instructors, and qualification or certification of drill and exercise controllers. The final rule will maintain the intent of the security orders and put in place requirements to meet the revised DBT by establishing the requirement for a cyber security program to protect any systems that if compromised, can adversely impact safety, security or emergency preparedness. Detailed analysis of the activities and procedural changes required by the rule are set forth in appendix A of this regulatory analysis.

(3) Potential change in the risk to the public from the accidental off-site release of radioactive material;

The rulemaking is intended to provide added assurance that the risk of offsite releases as a result of breaches in security at nuclear power plants is acceptably low and consistent with the NRC's Safety Goals. However, the reduction in risk to the public from offsite releases of radioactive materials has not been fully quantified because there is insufficient information and modeling to support such quantification (see Section 3.2).

(4) Potential impact on radiological exposure of facility employees;

The rulemaking will provide added assurance that nuclear industry workers are not subjected to unnecessary radiological or hazardous chemical exposures as the result of a breach in security that causes an accident leading to a release of radiation which workers then are exposed to as the result of mitigative and/or clean-up activities.

(5) Installation and continuing costs associated with the backfit, including the cost of facility downtime or the cost of construction delay;

The backfit analysis for the final power reactor security rule sets forth the NRC's estimate of the initial costs for implementing the major elements of the rule, and the ongoing costs and savings to the licensees. The estimated one-time industry net cost associated with the backfits will be approximately $115.71 million (or approximately $1.73 million for the average program), and the annually recurring cost will be approximately $38.65 million (or approximately $553,600 for the average program). Combining these initial and annual costs, this analysis estimates that the backfits associated with the power reactor security rule will cost industry approximately $590.23 million (present value, assuming a 7-percent discount rate) to $857.33 million (present value, assuming a 3-percent discount rate).

(6) The potential safety impact of changes in plant or operational complexity, including the relationship to final and existing regulatory requirements;

The power reactor security rule will make changes with respect to the design of a nuclear power plant. Specifically, the changes involve the following:

- The CAS and SAS must not be susceptible to both being lost to a single act;
- Advanced video surveillance systems must be installed; and
- The intrusion detection and assessment system must have an uninterrupted power source.

For new reactors:

- Both the CAS and the SAS must maintain functionally-equivalent capabilities.

These design changes do not affect all nuclear power plants because some currently meet these requirements. This rule is not expected to have a significant effect on facility complexity.

The rule will require modifications to training and "change control" procedures. These "costs" in terms of increased complexity in security procedures are detailed in appendix A of this regulatory analysis. The added complexity is not expected to be significant or to substantially impact licensees' operational practices or to result in substantial indirect costs.

(7) The estimated resource burden on the NRC associated with the backfit and the availability of such resources;

The rulemaking will result in a substantial increase in one-time expenditures of agency resources for the NRC to review and approve licensees' cyber security plans, and subsequently inspect implementation of licensee cyber security programs. Additionally, the NRC estimates that in the first year of implementation, it will spend 276 hours to revise implementation guidelines and inspection procedures. These activities will result in a one-time cost of approximately $2.60 million.

The rulemaking will not result in a substantial increase in annual expenditures of agency resources.

(8) The potential impact of differences in facility type, design or age on the relevancy and practicality of the backfit;

The security requirements in part 73 do not directly relate to the facility type, design or age. Although the benefits and costs attributable to the power reactor security rule will vary for a variety of site-specific reasons (e.g., facility layout, geography, choice of protective strategies), the NRC does not believe they will vary based upon the facility type, design or age.

(9) Whether the backfit is interim or final and, if interim, the justification for imposing the backfit on an interim basis.

The backfitting will be final.

The NRC finds that the backfitting contained in the final power reactor security rule, when considered in the aggregate, will constitute a substantial increase in protection to public health and safety and security. For reasons that were discussed in Section 3.2, it is not feasible to quantify the safety benefits of the rule. Nevertheless, NRC believes that the rule is warranted for several qualitative reasons. First, the final rule will provide assurance of licensees' capabilities to protect their sites against the DBT of radiological sabotage defined in § 73.1, in accordance with § 73.55(b). Second, there have been technological advances in intrusion detection systems that maintain an effective protection system and failure to implement these technologies could erode assurance that the physical protection system will perform as intended during a safeguards contingency. Third, the rule will increase the assurance that no single act could remove the functions of both the SAS and CAS. Fourth, the rule will increase licensees' security program effectiveness through procedures such as on-the-job training and increased qualification training. NRC believes that these factors represent a substantial increase in safety and that the rulemaking has merit on the basis of these stated qualitative reasons.

In light of the findings above, the NRC submits that the qualitative safety benefits of the power reactor security rule provisions that qualify as backfitting, considered in the aggregate, will constitute a substantial increase in protection to public health and safety and the common defense and security, and that the costs of this rule will be justified in view of the increase in protection to safety and security provided by the backfitting embodied in the rule.

4.3 Disaggregation

In order to comply with the guidance provided in Section 4.3.2 ("Criteria for the Treatment of Individual Requirements") of the Regulatory Analysis Guidelines, the NRC conducted a screening review to ensure that the aggregate analysis does not mask the inclusion of individual rule provisions that are not cost-beneficial when considered individually and not necessary to meet the goals of the rulemaking. Consistent with the Regulatory Guidelines, the NRC evaluated, on a disaggregated basis, each of the 25 new regulatory provisions expected to result in incremental costs or savings. Based on this screening review, the NRC staff has determined that each of the requirements is needed and is cost-justified relative to its qualitative benefits.

4.4 Safety Goal Evaluation

Safety goal evaluations are applicable only to regulatory initiatives considered to be generic safety enhancement backfits subject to the substantial additional protection standard at § 50.109(a)(3).[4] Some aspects of the rule may qualify as generic safety enhancements because they may affect the likelihood of core damage or spent fuel damage, which generally are the focus of a quantitative safety goal evaluation. However, the magnitude of this change is not readily quantifiable due to uncertainties discussed in Section 3.2 above. A more dominant effect of the rule is to reduce the probability of other types of damage associated with a wide array of acts of sabotage, although this effect is equally difficult to quantify. Because the change in safety associated with the rulemaking cannot be quantified, the regulatory changes cannot be compared to NRC's safety goals.

4.5 CRGR Results

This section addresses regulatory analysis information requirements for rulemaking actions or staff positions subject to review by the Committee to Review Generic Requirements (CRGR). All information that will be provided to the CRGR for information is presented in this regulatory analysis, or in the Federal Register notice for the final power reactor security rule. As a reference aid, Exhibit 4-4 provides a cross-reference between the relevant information and its location in this document or the Federal Register notice. Note that the rulemaking process was recently revised by Commission SRM dated October 25, 2007, and as a result, this information is provided to the CRGR for information only, not for review and approval.

[4] A safety goal evaluation is not needed, therefore, for new requirements falling within the backfit exceptions at 10 CFR 50.109(a)(4)(i)-(iii).

Exhibit 4-4
Specific CRGR Regulatory Analysis Information Requirements

CRGR Charter Citation	Information Item to be Included in a Regulatory Analysis Prepared for CRGR Review (information only)	Where Item is Discussed
IV.B(1)	Generic requirement or staff position as it is to be sent out to licensees. When the objective or intended result of a generic requirement or staff position can be achieved by setting a readily quantifiable standard that has an unambiguous relationship to a readily measurable quantity and is enforceable, the requirements should specify the objective or result to be attained rather than prescribing how the objective or result is to be attained.	Rule text in Federal Register Notice
IV.B(iii)	The sponsoring office's position on whether the action will increase requirements or staff positions, implement existing requirements or staff positions, or relax or reduce existing requirements or staff positions.	Regulatory Analysis, Section 4.1
IV.B(iv)	The method of implementation.	Regulatory Analysis, Section 6
IV.B(vi)	Identification of the category of power reactors or nuclear materials facilities/activities to which the generic requirement or staff position will apply.	Regulatory Analysis, Section 3.2.2 and 4.2
IV.B(vii) IV.B(viii)	If the action involves a power reactor backfit and the exceptions at 10 CFR 50.109(a)(4) are not applicable, the items required at 10 CFR 50.109(c) and the required rationale at 10 CFR 50.109(a)(3) are to be included.	Regulatory Analysis, Section 4.2
IV.B(x)	For relaxations or decreases in current requirements or staff positions, a rationale is to be included for the determination that (a) the public health and safety and the common defense and security will be adequately protected if the reduction in requirements or positions were implemented, and (b) the cost savings attributed to the action will be substantial enough to justify taking the action.	Federal Register Notice for the rule
IV.B(xii)	Preparation of an assessment of how the action relates to the Commission's Safety Goal Policy Statement.	Regulatory Analysis, Section 4.4

5. Decision Rationale

5.1 Regulatory Analysis

Relative to the “no-action” alternative, the final rule will result in a net cost estimated as approximately $592.84 million (total present value over a 30-year period), assuming a 7-percent discount rate, or approximately $859.93 million assuming a 3-percent discount rate. All of this cost will accrue to industry, except for approximately $2.6 million that will accrue to the NRC. The rule will result in one-time industry costs of approximately $115.71 million. This is equivalent to approximately $1.78 million for the average reactor site. The final rule language will generate annual industry costs of about $38.65 million ($594,600 per site). Offsetting this net cost, the NRC believes that the rule will result in substantial non-quantified benefits related to safety and security, as well as enhanced regulatory efficiency and effectiveness. The analysis presents these benefits in Section 4.1 of this document. Based on the NRC's assessment of the costs and benefits of the propose rule on licensee facilities, the agency has concluded that the final rule provisions will be justified.

The final rule will result in an annual impact to the economy of approximately $47.36 million (using a 7 percent discount rate, annualizing the one-time costs over 30 years, and adding these “annualized” one-time costs to the annual costs) or $44.38 (using a 3 percent discount rate). This final rule is therefore not a major rule as defined by the Congressional Review Act.

5.2 Backfit Analysis

The NRC conducted a backfit analysis of the power reactor security rule relative to the backfitting requirements in 10 CFR 50.109. Certain requirements of the final rule do constitute backfitting because they will result in the modification of or addition to systems, structures, components or design of a nuclear power plant, or the procedures or organization required to design, construct, or operate a facility. The measures constituting backfitting, in general, include establishing cyber security programs to protect computer systems; updating security plans and relevant procedures; enhancing intrusion detection and assessment system technologies in the CAS and SAS; developing and implementing safety/security interface procedures to avoid adverse safety/security interactions; extending armed security personnel requirements for vision, hearing, medical, and physical qualifications to unarmed security personnel; conducting on-the-job training for new armed and unarmed members of the security organization and drill exercises. These new measures meet the definition of a backfit because such efforts will be new and will be the result of additional or modified provisions in the NRC's current rules.

The NRC believes that the backfitting required by this rule is cost-justified for several qualitative reasons. First, the rule will provide additional assurance of licensees’ capability to protect the power reactor sites against assaults up to and including the DBT of radiological sabotage. Second, the rule will require uninterruptible power supplies and extension of the “no single act” criterion to key alarm station functions. In this regard the rule will also result in the deployment of certain technological advances in intrusion detection systems that are enhancements during

a safeguards contingency. Third, in recognition of advancing digital technology, the rule will maintain the intent of the security orders and put in place requirements for meeting the radiological sabotage DBT by establishing the requirement for a cyber security program to protect any systems that could, if compromised, adversely impact safety, security or emergency preparedness. Fourth, the rule will increase licensees' security program effectiveness through additional training and qualification measures, including safety/security interface, on-the-job training and armorer certification. NRC concludes that these factors represent a substantial increase in safety and that the rulemaking has merit on the basis of these stated qualitative reasons.

6. Implementation

This section identifies how and when the rule will be implemented, the required NRC actions to ensure implementation, and the impact on NRC resources.

6.1 Schedule

The final rulemaking will become effective on 30 days following publication in the Federal Register. It is expected that the final rule will be published in early, to mid, 2009. The final rule requires that within 180 days, 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 final rule. Those changes must be incorporated into their security plans, as necessary. In doing so, licensees are expected to follow the appropriate change processes described currently in § 50.54(p), § 50.90 or § 73.5. Section 73.54 requires licensees to submit a cyber security plan within 180 days of the effective date of the rule for NRC review and approval.

6.2 Impacts on Other Requirements

As discussed in Section 4.1, affected licensees will experience most of the impact of the revisions to 10 CFR part 73. The rulemaking will result in a substantial increase in one-time expenditures of agency resources for the NRC to review and approve licensees' cyber security plans, as well as subsequent inspections of licensee cyber security programs. Additionally, the NRC estimates that in the first year of implementation, it will spend 276 hours to revise implementation guidelines and inspection procedures. These activities will result in a one-time cost of approximately $2.60 million. However, the NRC does not expect that the rulemaking subsequently will result in a substantial increase in annual expenditures of agency resources.

Integrated Comment Responses Supporting Final Rule: Power Reactor Security Requirements

U.S. Nuclear Regulatory Commission
Office of Nuclear Reactor Regulation

June 2008

UNITED STATES NUCLEAR REGULATORY COMMISSION

POWER REACTOR SECURITY REQUIREMENTS

INTEGRATED COMMENT RESPONSES

The U.S. Nuclear Regulatory Commission (NRC) is amending the security requirements for nuclear power reactors. The security requirements being amended by the power reactor security rulemaking are: 10 CFR 73.55, 10 CFR 73.56, 10 CFR Part 73 Appendix B, and 10 CFR Part 73 Appendix C. Additionally, the NRC is adding three new requirements to Parts 50 and 73 respectively: 10 CFR 50.54(hh), 10 CFR 73.54, and 10 CFR 73.58. Finally, the rulemaking makes conforming changes to other sections of Part 73, Part 72, Part 50, and Part 52 to 1) ensure that cross-referencing between the various security regulations in Part 73 is preserved, 2) implement cyber security plan submittal requirements, and 3) preserve requirements for licensees who are not within the scope of this rule.

Following the terrorist attacks on September 11, 2001, the NRC conducted a thorough review of security to ensure that nuclear power plants and other licensed facilities continued to have effective security measures in place given the changing threat environment. Through a series of orders, the Commission supplemented the Design Basis Threat (DBT), as well as requirements for specific training enhancements, access authorization enhancements, security officer work hours, and enhancements to defensive strategies, mitigative measures, and integrated response. Additionally, in generic communications, the Commission specified expectations for enhanced notifications to the NRC for certain security events or suspicious activities.

As noted to recipients of the various Commission orders, it was always the Commission's intent to undertake a rulemaking that would codify generically applicable security requirements and update its power reactor security requirements, which had not been significantly updated for nearly 30 years. Thus, on October 26, 2006, the Commission proposed the Power Reactor Security Rulemaking. (71 FR 62664). The proposed rule was published for a 75-day public comment period and, in response to requests, the comment period was extended on two separate occasions (72 FR 480 and 72 FR 8951), finally closing on March 26, 2007.

The Commission received 48 comment letters. In addition, the Commission held two public meetings in Rockville, MD, and Las Vegas, NV on November 15 and 29, 2006, respectively, to solicit public comment. The NRC also held a third public meeting on March 9, 2007, to facilitate stakeholder understanding of the proposed rule requirements and thereby result in more informed comments on the proposed rule provisions.

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 NRC had decided to provide additional detail. The supplemental proposed rule also proposed to move from these requirements from Appendix C to Part 73 in the proposed rule to Section 50.54 in the final rule. Three petitions for rulemaking were also considered as part of the power reactor security rulemaking.

The Commission's responses to the received public comments are discussed below.

General Issues and Specific Questions
Responses to Public Comments

Comment Summary:
Several commenters generally supported this rulemaking on the basis that it is important to codify the requirements that were imposed on industry after September 11, 2001. In particular, the commenters pointed to the Energy Policy Act of 2005 (EPAct 2005) requirements as those that need to be codified. Other commenters pointed to specific elements of the rule that they support, such as the inclusion of the requirement to defend against spent fuel sabotage, expanding the licensee's security obligations to include the owner controlled area (OCA), and the use of enhanced weapons by security officers. The commenters also stated that, if constructed properly, the new rules would not be an undue burden to licensees.

NRC Response:
The NRC agrees with commenters that support the security rulemaking. The NRC notes that while the supporters agreed with elements of this rulemaking, the objectives for the rulemaking were to: make generically applicable security requirements imposed by Commission orders issued after the terrorist attacks of September 11, 2001, based upon experience and insights gained by the Commission during implementation; fulfill certain provisions of EPAct 2005; add several new requirements that resulted from insights from implementation of the security orders, review of site security plans, and implementation of the enhanced baseline inspection program and force-on-force exercises; update the regulatory framework in preparation for receiving license applications for new reactors; and give consideration to three petitions for rulemaking during the development of the final rule requirements. No changes to the final rule or supporting SOC were made as a result of this comment.

Comment Summary:
Commenters opposed the rulemaking for various reasons. Commenters believe the rulemaking is designed to codify an inadequate status quo, while other commenters did not believe the rulemaking incorporated certain provisions of EPAct 2005 relating to the conduct of security-based drills and conflict of interest. Other commenters expressed concern over what are viewed as weakened requirements that govern MOX fuel. On the other hand, there were several commenters who stated that the proposed language creates several new requirements which will impact licensees' current plans, which have already been approved by the NRC, and these new requirements could divert security attention away from active defense and cause licensees to incur significant additional expenditures. Commenters expressed concern regarding the broad language used for some requirements, and stated that the NRC should revise the proposed rule to minimize misinterpretations and to avoid the inadvertent creation of new requirements.

NRC Response:
The NRC disagrees with the comments that suggest this rulemaking codifies the status quo. As discussed in the comment response above, this rulemaking goes beyond codifying current practices and instead incorporates lessons-learned from the implementation of the security orders, review of site security plans, and implementation of the enhanced baseline inspection program and force-on-force exercises. The NRC disagrees that the rulemaking does not incorporate security-based drills and conflict of interest provisions of EPAct 2005. The final rule

performance evaluation program requirements, relocated to Appendix B VI.C.3, address both of these requirements. The NRC disagrees that the MOX fuel requirements are weakened security requirements and instead, the NRC adjusted the requirements governing MOX fuel to maintain adequate security for this fuel based on the relevant security issues. With regard to the commenters who expressed concern that the rule language is too broad, or that new requirements are being introduced that could divert attention, the NRC, where possible (within the limitations of SGI), revised the language and moved some provisions to address these issues. These issues are addressed in specific comment responses for each requirement.

Comment Summary:
Many of the comments from industry identify as a primary concern with the proposed power reactor security rulemaking that the Commission did not simply "codify" requirements contained in the various security orders issued during the several years after September 11th. The Nuclear Energy Institute (NEI), for example, asks, "Why were these new provisions not imposed in 2003 when the Commission issued orders to bolster security in light of the increased threat environment?" There are a number of justifications that clearly support the Commission's proposal of security measures in this proposed rule that exceeded what was previously imposed by Order.

NRC Response:
As an initial matter, the suggestion that "…the primary goal of the rulemaking was to codify the post-9-11 orders into security regulations," as stated by several industry commenters, is misleading and arguably inconsistent with the NRC's obligations under the Administrative Procedure Act (APA). First, as stated in the proposed rule, one goal of this rulemaking was to "make generically applicable security requirements imposed by Commission orders," (71 FR 62664), but that was by no means the only goal. As clearly stated, the Commission also intended to implement "several new requirements that resulted from insights from implementation of the security orders, review of site security plans, and implementation of the enhanced baseline inspection program and force-on-force exercises." These insights were obviously not available to the Commission when it issued the original set of security orders in 2002 and 2003, and it would be a serious opportunity wasted if the Commission did not attempt to improve the rule with the benefit of these lessons.

In addition, another key objective of this rulemaking was to "update the regulatory framework in preparation for receiving license applications for new reactors," (71 FR 62664). The current security regulations have not been substantially revised for nearly 30 years. Prior to September 11th, the Commission had already undertaken an effort to revise these dated requirements, but that effort was delayed for obvious reasons. Thus, this rulemaking picks up where the NRC's previous pre-September 11th efforts left off. It is important to keep in mind that this rulemaking will have a much wider impact than simply its effect on current reactors. New reactor applicants will need clearly articulated requirements that the former regulation could not provide. Additionally, the revisions to this rule were intended to provide it with needed longevity, so that the NRC would not be obligated to return to the rulemaking process in the next several years for failure to be forward thinking and anticipate future developments or needs in physical protection.

As a legal matter, the APA prevents the agency from simply "codifying" orders into a regulation, but instead requires that our rules are published for public comment in the Federal Register and be subjected to a public process. To suggest that the agency could simply take a set of requirements it imposed as interim measures under extraordinary circumstances and make them into a generic set of regulations is inconsistent with those legal obligations.

In addition, the initial Interim Compensatory Measure (ICM) Order (EA-02-026) was issued on February 25, 2002, (67 FR 9792) – a mere 5 months after the events of September 11th. Though several additional security orders were issued subsequent to the ICM Order, the ICM Order contained the bulk of security requirements. However, the ICM Order and the letter transmitting the Order were very clear: the measures imposed by Order were "interim requirements" and that they would remain in effect "…until the Commission determines that other changes are needed following a comprehensive re-evaluation of current safeguards and security programs," (67 FR 9792). It was always the Commission's intent to revisit the adequacy of these interim security measures through a comprehensive rulemaking process that took advantage of stakeholder input, Commission experience, and the benefit of hindsight. The proposed rule reflected this effort, and therefore included a number of "new" requirements that went beyond the Order. The agency is not bound to a set of requirements it developed to the best of its ability and which it believed were prudent at the time, but nevertheless developed under extraordinarily difficult circumstances.

In sum, though a key objective of this rulemaking was to use the requirements of previous security orders as a baseline, the Commission by no means intended to simply "codify" those orders.

Comment Summary:
One commenter stated that the rule broadly imposes requirements on "any area" or "all areas" when previously it specified the specific area. Similarly, the commenter said the rule imposes requirements on "any barrier established to meet the requirements of this section" when the requirement is clearly not applicable to all such barriers. The same commenter stated that the NRC has admitted that the threat environment has not changed since the EPAct of 2005, but has still used the changing threat environment as justification for adding new requirements throughout this rulemaking.

NRC Response:
The NRC addressed the commenter's concern regarding requirements that are broadly imposed on all areas (of the facility) by revising the final requirements to be more area specific. The NRC agrees with the commenter that the basis for new requirements in this rulemaking (new requirements that go beyond previously imposed post September 11 order requirements) is not a changing threat environment. Instead new requirements are justified as cost-justified safety enhancements per the criteria in 10 CFR 50.109(a)(3). Changes to implement this response are in the specific requirements sections.

Comment Summary:
Several commenters noted that the following words and phrases need to be more clearly defined: entrance, unauthorized activities, unauthorized materials, significant core damage, spent fuel sabotage, early detection, technology, computer technology, video technology, components, and equipment.

NRC Response:
In the specific areas where stakeholders suggested that terms should be defined, NRC decided to address these issues by tightening the associated requirement (within the limitations of SGI), and/or supporting the requirements with guidance that addresses the issue. Refer to the comment responses associated with each of the relevant requirements.

Comment Summary/Specific Request for Feedback:
The NRC solicited public comment on a number of specific issues, but received input on only one of these specific issues. Specifically, the NRC 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. In response, 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 control system cyber security program is dependent on the scope and findings and discussed the technologies and programmatic approaches that can be pursued to augment NEI 04-04, “Cyber Security Program for Power Reactors,” recommendations.

NRC Response:
The NRC appreciates this feedback, and focused considerable attention on cyber security requirements in developing the final rule requirements. The cyber security guidance (SGI) developed by NRC goes into greater detail than the current version of NEI 04-04 and it recognizes both the changing technology and the nature of the cyber threat.

Regulatory Analysis Issues
Responses to Public Comments

Comment Summary:
Commenters indicated that the regulatory analysis underestimates the costs of all the new requirements in the proposed rule, and that the one-time and annual costs for licensees were skewed.

NRC Response:
The NRC agrees in part. Regarding the cost estimates supporting the final rule regulatory analysis, it is the NRC's objective to make decisions based on complete and accurate cost information. This objective is particularly important for this rulemaking since the costs are an integral part of the decision to backfit the new requirements under § 50.109(a)(3). Where there was information indicating that the cost estimates were low either due to information provided from external stakeholders or due to comments that revealed that the provisions involved more effort to implement than originally stated in the proposed rule regulatory analysis, the NRC revised the costs estimates consistent with the spirit of this comment. Refer to the final rule regulatory analysis for specific changes.

Comment Summary:
A commenter indicated that the fundamental approach used for impacts was to multiply the cost of the impact by the anticipated number of sites affected, and then divide by the total number of sites to get a per site impact. The commenter argued that this approach is misleading. The commenter also indicated that the regulatory analysis identified the new requirements, yet in many instances only a percentage of sites were assumed to be impacted. The commenter asked how a new requirement can only apply to a percentage of the 65 operating reactors.

NRC Response:
The NRC used the standard approach for calculating costs/impacts and averaging those costs on a site-specific basis. The NRC recognizes that in some cases (i.e., where there is a small percentage of sites that would incur an impact) this approach may be somewhat misleading. Where applicable, the NRC revised the final regulatory analysis to note where these situations exist, and provided the impacts for the limited number of sites that the NRC estimates would be impacted.

Regarding why only a small percentage of sites are impacted by a new requirement, the NRC attempted to account for the current sites that already have the feature implemented (even though it is technically not a requirement) so that a true estimate of the requirement impact was provided. Recognizing that all new requirements have some impact on licensees (regardless of whether the licensee is currently implementing a similar requirement as a result of a security plan commitment), the NRC added an additional cost to the final rule regulatory analysis that addresses the impact that licensees would incur. This impact is to estimate the costs associated with an overall review of security plans and implementing procedures to update them to the new governing requirements.

Comment Summary:
The commenter discussed that not all new requirements were evaluated by the regulatory analysis. The commenter stated that there are numerous examples where the rule language

has been moderately to extensively changed, and are not justified or accounted for in the regulatory analysis. The commenter identified what he considers the “new” requirements in the proposed rule.

NRC Response:
Each of the identified new requirements were in 10 CFR 73.55. With regard to the specific list of requirements, in all cases except one, the NRC has either revised the associated final rule requirement language to resolve the issue (i.e., the NRC did not intend that the listed item be a new requirement and so revised the language to remove the unintentional requirement) or, where a language revision is not possible (due to the limitations of SGI), the NRC has issued draft supporting guidance that clarifies the intent for the listed requirement such that it should no longer be viewed as a new requirement. The only exception is the requirement that touches upon video assessment/playback where the NRC is imposing a new requirement. This new requirement is addressed in both the proposed and final rule regulatory analysis.

The NRC does note that there are a number of new requirements in the final rule that are current practices. These practices have been implemented throughout industry following an NRC approved NEI template that incorporated the practices into security plans which the NRC reviewed and approved following the issuance of the post 9/11 orders. Requiring these current practices does impose an impact on licensees, and the NRC accounts for that impact in the final rule regulatory analysis (i.e., the estimated impact is to account for the review and revision of plans and supporting procedures to reflect the new requirements).

Comment Summary:
During a public meeting, a commenter asked if the NRC had a matrix that would show how many new requirements there are in the proposed rule.

NRC Response:
As suggested during the public meeting, the regulatory analysis is the document that shows new requirements and their costs.

10 CFR 50.54(hh)
Responses to Public Comments

Comment Summary:
The commenters indicated that three statements in the section by section analysis (supporting 10 CFR 50.54(hh)(1)) are new expectations. This comment referred to the description that indicated licensees would need to 1) determine how much time is necessary to evacuate their protected areas, 2) validate the accuracy of that determination using no-notice drills, and 3) incorporate the lessons learned from those drills into the site-specific procedures. Additionally, the commenters stated that suspension of security measures via 10 CFR 50.54(x) would need to be considered when conducting no-notice protected area evacuations.

NRC Response:
The Commission agrees in part with this comment. 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 10 CFR 50.47(b)(14) and Appendix E to Part 50, Section (IV)(F)(g). Depending upon the methodology used to conduct the analysis, it may not be necessary to suspend security measures pursuant to 10 CFR 50.54(x) or 10 CFR 73.55(p), as applicable. The Commission revised the SOC language to clarify NRC intent.

Comment Summary:
A commenter stated that the requirement in proposed 10 CFR 50.54(hh)(1)(ii) “Maintenance of continuous communication with applicable entities” could potentially be a resource and task burden for site response organizations depending on the duration of the pre-event period. The commenter suggested that this requirement be revised to read: “Allow for periodic updates during the pre-event period as necessary to the applicable entities.” Another stakeholder with a similar concern suggested “Maintenance of communications with applicable entities as necessary and as resources allow.”

NRC Response:
The NRC agrees in part with these comments. The goal is for threat notification sources to be able to communicate pertinent information to licensees, not to unnecessarily burden licensee personnel with redundant requirements. As a result, the Commission changed 10 CFR 50.54(hh)(1)(ii) to read, “Maintenance of continuous communication with threat notification sources”. Examples of threat notification sources are 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. If a licensee encounters a situation where multiple threat notification sources (e.g., FAA, NORAD and NRC Headquarters Operations Center) are providing the same threat information, licensees would only be required to maintain continuous communication with the NRC Headquarters Operations Center. The Commission also revised the SOC language to clarify the purpose of this requirement.

Comment Summary:

The commenter stated that the requirement in proposed 10 CFR 50.54(hh)(1)(iii) is redundant with existing requirements in 10 CFR part 50 Appendix E and that the NRC needs to be mindful of redundancy issues and provide clarifying language when the Emergency Planning regulations are revised to acknowledge that the provision is already addressed in the imminent threat procedure.

NRC Response:
The Commission disagrees with this comment. The intent of the rule 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 rule text implied. Consequently, the Commission replaced the term "Notifications of" with "Contacting" in the rule text and SOC language.

Comment Summary:
The commenter indicated that the requirement in proposed 10 CFR 50.54(hh)(1)(iv) that states "onsite protective actions to enhance the capability of the facility to mitigate the consequences of an aircraft impact" appears to be redundant with a portion of the Emergency Preparedness draft Preliminary rulemaking (paragraph I "Onsite Protective Actions During Hostile Action Events") since an aircraft threat would constitute a hostile action. The commenter stated that NRC needs to be mindful of redundancy issues and provide clarifying language when the Emergency Planning regulations are revised to acknowledge that the provision is already addressed in the imminent threat procedure.

NRC Response:
The Commission agrees is part with this comment. Paragraph 50.54(hh)(1)(iv) pertains to operational actions that licensees can take to mitigate the consequences of an aircraft impact; the NRC did not intend this requirement to include emergency preparedness-related protective actions. The Commission removed the term "protective" from the rule text to eliminate this ambiguity.

Comment Summary:
The commenter declared that the requirement in proposed 10 CFR 50.54(hh)(1)(v) that states, "…measures to reduce visual discrimination of the site relative to its surroundings or individual buildings within the protected area," should be deleted. The commenter believes that this measure was previously deemed to be prohibitively expensive, and that imposing the requirement at this time requires a backfit analysis.

NRC Response:
The NRC disagrees with this comment. As explained in the SOCs, licensees would be required to either utilize centralized lighting controls, or in the absence of centralized controls, develop prioritized routes that allow personnel to turn off different sets of lights depending on available time, when appropriate. For the first option, the NRC is aware that the resources (i.e., centralized lighting controls) are already available for some licensees; the second option is a reasonable alternative for those licensees without centralized controls. Consequently, neither option requires a "prohibitively expensive" capital investment or a backfit analysis. The rule language and the SOCs were not revised.

Comment Summary:
The commenter stated that the proposed 10 CFR 50.54(hh)(1)(vi) seems to add new requirements and terminology. The commenter notes that "rapid reentry" is a new term, and

that it is not necessary for all personnel initially evacuated from the protected area or all offsite responders to rapidly reenter/enter the protected area. The commenter suggests that "rapid reentry should apply only to personnel essential to mitigate the event.

NRC Response:
The Commission agrees with this comment. The intent of this requirement is to ensure appropriate onsite personnel and offsite responders are not unnecessarily delayed by routine protected area entry processing during an event. The Commission changed 10 CFR 50.54(hh)(1)(vi) to read, "…rapid entry into site protected areas for essential onsite personnel and offsite responders who are necessary to mitigate the event…". The Commission also revised the SOCs to clarify the purpose of this requirement.

Comment Summary:
The commenter stated that the requirement in proposed 10 CFR 50.54(hh)(1)(vi) discussing the pre-staging and dispersal of equipment and personnel looks like it is redundant with a provision in the draft Emergency Preparedness preliminary rulemaking (which the commenter describes). The commenter stated that the NRC needs to be mindful of redundancy issues and provide clarifying language when the Emergency Planning regulations are revised to acknowledge that the provision is already addressed in the imminent threat procedure.

NRC Response:
The NRC agrees with this comment. The term, "pre-staging", often connotes repositioning of personnel or equipment during the planning phase in preparation for an event. The Commission intended to require licensees to disperse essential personnel and equipment to pre-identified locations after receiving potential aircraft threat notifications, but prior to actual aircraft impacts, when possible. The Commission revised the rule text and SOC language. The draft Emergency Preparedness rule will reference 10 CFR 50.54(hh)(1)(vi), as appropriate, to avoid redundant requirements.

Comment Summary:
The commenter stated that the proposed 10 CFR 50.54(hh)(2)(i) discusses the need for licensees to have fire fighting strategies for dealing with loss of large areas of the plant due to explosions and fires and that this provisions looks like it is redundant with a provision in the draft Emergency Preparedness preliminary rulemaking (which the commenter describes). The commenter stated that the NRC needs to be mindful of redundancy issues and provide clarifying language when the Emergency Planning regulations are revised to acknowledge that the provision is already addressed in the imminent threat procedure.

NRC Response:
The Commission agrees with the intent of the comment, that there should not be redundant requirements. However, in this instance, the Commission does not believe there is an overlap. Paragraph 50.54(hh)(2)(i) provides the requirements for response to loss of large areas of the plant due to explosions or fires. The proposed Emergency Preparedness rule contains requirements for drills and exercises that would test this response capability.

Comment Summary:
The commenter stated that the final rule should include an applicability statement similar to the following: "This section does not apply to a nuclear reactor facility for which the certifications required under 10 CFR 50.82(a)(1) have been submitted." The commenter believes that it is inappropriate that 10 CFR 50.54(hh) should apply to a permanently shutdown, defueled reactor

where the fuel was removed from the site or moved to an Independent Spent Fuel Storage Installation.

NRC Response:
The NRC agrees. The requirements of 10 CFR 50.54(hh) do not apply to any current facilities in decommissioning, and the requirements do not need to be applicable to future decommissioning facilities for which certifications will be filed under 50.82(a)(1) or 52.110(a)(1). The final rule has been revised to reflect this comment.

Comment Summary:
The commenter believes the timeframe on which the verification required by 10 CFR 50.54(hh)(1)(i) is based is a vital consideration for protective response. The commenter states that "verification" may be an issue that the NRC and its licensee might wish to keep secure. Additionally, the commenter indicated that the timeframe in which a response must be verified must be clear and it is not currently clear.

NRC Response:
The Commission agrees in part with this comment. The verification timeframe is important, and that timeframe should be minimized as much as possible. To that end, on June 25, 2007, the NRC issued Security Advisory 2007-01, Revision 1, which outlines the call verification process between the NRC and its power reactor licensees. The document number is ML070790129, and it is available to the public via the NRC's Agencywide Documents Access and Management System. The rule text and the SOC language were not revised.

Comment Summary:
The commenter, based on its experience, believes that Emergency Planning exercises must assume the potential for communication failures or inadequate communications, and must resolve the shortcomings via exercises, planning, and technology. This comment is provided in reference to 10 CFR 50.54(hh)(1)(ii).

NRC Response:
The Commission disagrees with this comment. This requirement in 10 CFR 50.54(hh)(1)(ii) exists to ensure that threat notification sources are able to communicate pertinent information to licensees. As a result of a previous comment, the Commission revised the rule text to clarify that purpose. The remainder of this comment is beyond the scope of this rule. The requirement is not related to emergency preparedness exercises, and this rule requires no test of the emergency notification systems, although other parts of the regulations do (e.g., Appendix E to Part 50). The rule text and the SOC language were not revised.

Comment Summary:
In reference to 10 CFR 50.54(hh)(1)(iii), the commenter reiterates the concern that telecommunications remains an unresolved issue, and also states that another issue of communications with on and offsite personnel and response organizations is the potential that these personnel will immediately notify their families and friends, creating severe problems in Emergency Planning that could exacerbate the sheltering and evacuation scenarios.

NRC Response:
The Commission disagrees with this comment. It is not clear how the commenter would like the rule to be revised. This particular requirement enables offsite response organizations to take actions deemed appropriate in advance of an onsite impact, which may increase the

effectiveness of the offsite response. The impact on emergency planning is beyond the scope of this requirement. Accordingly, the rule text and the SOC language were not revised.

Comment Summary:
In reference to 10 CFR 50.54(hh)(1)(iv), the commenter states that the NRC needs to recognize that the consequences (in terms of offsite releases) of an air attack are a real possibility. As an example the commenter notes that the NRC has not detailed how a radioactive fuel pool fire (from an air attack) would be addressed.

NRC Response:
The Commission agrees in part with this comment. The NRC recognizes there could be consequences as a result of a successful aircraft attack on a power reactor facility; therefore, 10 CFR 50.54(hh) was developed to address those consequences. However, details on specific site mitigative actions are not available to the general public. The rule text and the SOC language were not revised.

Comment Summary:
In reference to 10 CFR 50.54(hh)(1)(v), the commenter questions the sincerity of this requirement indicating that this would be virtually impossible for reactor facilities, and that the locations of reactor facilities are well known.

NRC Response:
The Commission disagrees with this comment. As explained in the SOCs, licensees would be required to either utilize centralized lighting controls, or in the absence of centralized controls, develop prioritized routes that allow personnel to turn off different sets of lights depending on available time, when appropriate. Although the locations of power reactor sites may be well known or a hostile aircraft may be equipped with global-positioning equipment, some visual discrimination of the site or of specific buildings within a protected area may be necessary to conduct a successful attack. Consequently, it is appropriate for power reactor licensees to use readily-available resources to hinder nighttime visual discrimination to the extent possible. The rule language and the SOCs were not revised.

Comment Summary:
In reference to 10 CFR 50.54(hh)(1)(vi) and (vii), the commenter suggests that the NRC should assume that 10 to 25 percent of the personnel who evacuate the site will not return (due to the concern that these people will want to see that their families are safe). The commenter also indicates that some of the personnel from offsite agencies will not respond.

NRC Response:
The Commission disagrees with this comment. The rule does not assume any particular measures or personnel availability that would have to be included in licensee procedures. Licensees are responsible for determining how they will address a particular situation. Even though the rule requires consideration of the recall of site personnel, it does not specifically require that site personnel actually be recalled for an event, only that, if licensees determine that recalling such individuals is necessary to accomplish their objectives, that their procedures are documented and maintained. Even if the rule were to require recalls, it is mere speculation to assume that site personnel would not perform their duties in accordance with licensee procedures, and the Commission would have no basis to impose an arbitrary limitation on personnel who would normally be counted on to implement the licensees' plans. The rule text and SOC language were not revised.

Comment Summary:
In reference to 10 CFR 50.54(hh)(2)(i), the commenter believes that a radioactive fuel pool fire would not be exterminated for days, and that fire fighters are generally not trained for these types of events. As a result, the commenter believes that emergency planning scenarios account for situations where the strategies and guidance do not work and plan accordingly.

NRC Response:
The Commission considers this comment to be beyond the scope of this rule since this rule does not require the testing of specific fire-fighting procedures during emergency planning exercises. The procedures required by this rule are not intended to address any particular scenario, but rather to ensure that a licensee is capable of addressing a wide variety of situations that would result in the loss of large areas of the plant due to explosions or fire. No changes were made to the rule or supporting statement of considerations.

Comment Summary:
In reference to 10 CFR 50.54(hh)(2)(ii), the commenter indicates that this section is not clear and believes that if the NRC is sincere about strengthening radioactive fuel sites, then the NRC should require that pools and cask storage facilities be within containment.

NRC Response:
This comment is beyond the scope of this rulemaking. The Commission has already provided its position on the need for physical protection of spent fuel for aircraft attacks as part of the issuance of the final Design Basis Threat (DBT) rule (72 FR 12705, March 19, 2007). The NRC's position remains unchanged. No changes were made to the rule or supporting statement of considerations.

Comment Summary:
In reference to 10 CFR 50.54(hh)(2)(iii), the commenter does not believe that the NRC is sincere with regard to the need to harden fuel pools and fuel storage facilities. Additionally, the commenter does not believe that the NRC has done detailed engineering analyses of airliner crashes. The commenter indicates that the NRC has not taken seriously the suggestions of stakeholders that are intended to address aircraft attacks, and the commenter believes that NRC and its licensees do not really believe that an aircraft attack could result in offsite releases.

NRC Response:
This comment is beyond the scope of this rulemaking. As stated above, the NRC has already provided its positions on the need for physical protection of spent fuel for aircraft attacks as part of the issuance of the final DBT rule. The stakeholder's comment implies that NRC should revisit that decision including the engineering work performed to reach the NRC position. The NRC is not reconsidering its position in response to this comment. No changes were made to the rule or supporting statement of considerations.

Comment Summary:
The commenter notes that the top of page FR 19447, in the third column, the SOC states "…could be any number of design basis or beyond design basis threat events." The commenter states that since the aircraft impact is a beyond design basis event and the effects from that event are addressed under the aircraft impact rule then the design enhancements to address that event are just "safety enhancements."

The commenter indicates that this is how the SOC characterizes the mitigation of the aircraft impact effects and that they are not needed for "adequate protection." So the commenter reasons that the effects from the events covered by 10 CFR 50.54(hh)(2) would be events within the design basis threat and would be effects from a large area fire that effects a substantial portion of the plant. Following this logic, the commenter states that since there is no accelerant feeding this postulated fire and there are limited combustibles in a nuclear power plant, it is very difficult to conceive of a fire of this nature that could pose a threat to cooling capabilities.

The commenter believes that the rule needs to bound the area to be considered to either one Appendix R fire area or one Appendix R area and the adjacent areas on the same elevation. This is also true of large explosions created by the DBT. These explosions would be limited in the amount of damage inflicted to the plant because of the limited amount of explosives and would not involve substantial portions of the facility. The commenter then proceeds to state that this rule needs to be focused on security beyond design basis events and should require generic mitigative capabilities that can bound several events. It does not need to cover design basis events within the scope of the Design Basis Threat. Protective strategies developed under 10 CFR 73.55 are in place to protect cooling functions from the threats within the DBT.

Another commenter stated that 10 CFR 50.54(hh)(2) needs to focus on the site response to beyond design basis events and should require generic mitigative capabilities that can bound severe events. The rule need not cover events within the scope of the DBT, those are addressed by 10 CFR 73.55, so the rule should address events which cause a large area fire or impact a substantial portion of the plant. The commenter noted that nuclear power plant fire protection designs that comply with the requirements of 10 CFR 50.48 ensure that multiple safety divisions are not degraded or made inoperable from design basis fires. The commenter provided additional information concerning combustibles to support this conclusion.

NRC Response:
The NRC structured 10 CFR 50.54(hh) and the aircraft impact assessment rule to be complementary. First, the NRC notes that both sets of requirements are both addressing beyond design basis events. The 10 CFR 50.54(hh) requirements address a range of beyond design basis events that would include aircraft impacts, whereas the aircraft impact assessment requirements focus specifically on aircraft impacts.

With regard to the fires that the mitigative measures in 10 CFR 50.54(hh) are to address, these are fires that may be beyond the design basis Appendix R type fires. The Commission agrees with the commenter that the current fire requirements are adequate to address fires within the design basis of the facility, including fires that result from the DBT. However, it is the Commission's position that the requirements in 10 CFR 50.54(hh) provide reasonable assurance of adequate protection of public health and safety by requiring mitigative strategies for a range of beyond design basis accidents. In this sense, the requirements imposed by 10 CFR 50.54(hh) are similar to the evolution of other programs (some regulatory requirements and some voluntary industry initiatives) related to the mitigation of beyond design basis events (e.g., emergency operating procedures, severe accident management guidelines, severe accident features).

Comment Summary:
The Commission asked for stakeholder feedback on two questions in the 10 CFR 50.54(hh) Federal Register Notice. In the first question, the Commission asked whether there should be

language added to the proposed 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). The commenters indicated that (hh)(1) should be focused on a limited set of beyond design basis events; namely beyond design basis security events. The commenters also noted that the proposed paragraph (hh)(2) has no such limit and is currently unbounded such that the definition of large areas of the plant due to explosions or fire could be expanded to many beyond design basis events. By limiting the rule requirements to a generic set of beyond design basis security events, then strategies and procedures can be developed to focus on the restoration of capabilities needed for mitigating the effects from these events. The commenters then noted that the same restoration capabilities could then be utilized for many other events that were not in the generic set since they would be based on restoration of the stated cooling capabilities in the rule.

NRC Response:
The intent of the requirements in 10 CFR 50.54(hh) is to ensure that licensees have formulated mitigating strategies for the potential loss of large areas of the plant and the related potential loss of a variety plant equipment usually relied on to fulfill safety functions. Although the mitigating strategies do not, in and of themselves, ensure that a plant would survive all conceivable events without core damage, the development of plans and alternate means of fulfilling safety functions does serve to provide added assurance for the protection of the public health and safety. Whereas this requirement would not likely have been discussed in the context of adequate protection in the absence of concerns about security events, the mitigating strategies also serve to provide added protection for non-security events associated with the loss of plant equipment due to events such as fires or explosions. The language of 10 CFR 50.54(hh)(2) is, therefore, maintained to be more broad and not put into the context of beyond design basis security events. The Commission would not foresee changes in the mitigating strategies implemented at operating reactors or being developed for new reactors as a result of the current language in 10 CFR 50.54(hh)(2).

Comment Summary:
In the second question that the Commission asked for stakeholder feedback, the Commission requested input on what would be the most effective and efficient process to review the applicants' and licensees' procedures, guidance and strategies developed and maintained in accordance with 10 CFR 50.54(hh)(1) and (hh)(2). In response, commenters indicated that the procedures developed to comply with 10 CFR 50.54(hh)(1) will not be available at the time of a license application. These procedures are operations procedures. These procedures would be developed late in the construction of the plant and, along with other operations procedures, should be available for review prior to fuel load. The actions contained within these procedures would not be needed until fuel load when an aircraft threat would be present, so the most appropriate and efficient process for the Commission is to review these procedures as part of the review of operations procedures. The Commission would then review these procedures and strategies as part of their standard construction inspection programs at the construction site.

The commenters then stated that the process for implementing 10 CFR 50.54(hh)(2) would involve Emergency Operating Procedures, Severe Accident Mitigation Guidelines, Extreme Damage Mitigation Guidelines, or other similar guidelines. The strategies that would be developed for addressing (hh)(2) would not be available until all these procedures and guidelines have been developed because they will take credit for some of that guidance. The commenters, likewise, stated that these strategies should be available for NRC review just prior to fuel load and the most appropriate and efficient process for the NRC is to review these

procedures and guidelines as part of the review of operations procedures and beyond design basis guidelines. The commenters stated that the Commission should not review these documents as part of a combined operating license application but the review should be incorporated into the onsite procedural and guideline reviews prior to fuel load.

Additionally, the commenters stated that the NRC need not, and should not impose an additional requirement in 10 CFR 50.34 and 10 CFR 52.80 to include these materials, noting that the information will not be available and that Commission has already reached a conclusion that there would be a license condition on this matter by putting these provisions into 10 CFR 50.54. Finally, the commenters noted that if the NRC requires 10 CFR 50.54(hh) information as part of the licensing process, it should be in the form of a brief summary program description.

NRC Response:
For new reactors, the requirements of 10 CFR 50.54(hh)(1) are largely met through the development of operating procedures that will not be developed at the time of a combined license application. In addition, the requirements of 10 CFR 50.54(hh)(1) are prescriptive and are comparable to or exceed the level of detail that would be expected for an operational program in a combined license application. For this reason, the Commission agrees that additional descriptions are not needed for combined license applications and has not included a regulatory requirement for such information to be included in applications.

Regarding the requirements of 10 CFR 50.54(hh)(2), the Commission views the mitigating strategies 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 prior to 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. Because the Commission finds that the most effective approach is for the mitigating strategies, at least at the programmatic level, to be developed prior to construction and reviewed and approved during licensing, a requirement for information has been added to 10 CFR 52.80, “Contents of applications; additional technical information,” and 10 CFR 50.34, “Contents of construction permits and operating license applications; technical information.”

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

Comment Summary:
Two commenters suggested that NRC should change the term “emergency preparedness” to “emergency response.” One of the commenters explained that NEI 04-04 “Cyber Security Program for Power Reactors” Revision 1, which is endorsed by the NRC, covers emergency response systems, but not emergency preparedness systems. The commenters believed that by changing the wording in the proposed rule, the NRC will avoid confusion.

NRC Response:
The NRC disagrees. The NRC revised the final rule to clarify the general performance objective for the protection of digital computer and communication systems and networks against cyber attacks. The Commission added language to clarify the intended scope of what is meant by the proposed rule "safety, security, and ***emergency preparedness***". The final rule retains the term "emergency preparedness". The term Emergency Preparedness Systems, is used consistent with 10 CFR Part 50, Appendix E terminology. The equipment embodied within these "preparedness" systems includes a wide variety of plant monitoring systems, protection systems, and plant communications systems used during an emergency event. The term "Emergency Response Systems" is used more specifically to refer only to the "emergency response data system" or ERDS. The ERDS is very specifically identified in 10 CFR Part 50 as the system which provides a data link that transmits key plant parameters. Using the definitions in Appendix E, the term "emergency preparedness" is the most appropriate term because it includes the on-site and off-site emergency communications systems.

Comment Summary:
One commenter stated that there are several ongoing industry efforts addressing cyber security. These efforts include ISA SP99, NERC CIP, and NEI 04-04. Although the proposed rule is supposed to be consistent with ongoing industry efforts, the commenter explained that only ISA SP99 specifically addresses industrial control systems including those used in commercial nuclear power plants.

NRC Response:
The NRC agrees that the requirements of this section are intended to be consistent with ongoing NRC and industry efforts. The NRC has developed draft regulatory guidance deemed appropriate to satisfy the requirements of this section of the final rule. In developing draft Regulatory Guide (DG-5022) the NRC considered all available professional literature for applicability.

Comment Summary:
One commenter noted that the CAS and SAS have cyber connections, but the proposed rule does not include any requirements to address the CAS and SAS cyber connections.

NRC Response:
The NRC disagrees. The proposed rule 73.55(m)(1) used the phrase "...which if compromised would likely adversely impact safety, *security,* and emergency preparedness." The CAS and SAS connections are inclusive to term "security". The NRC has revised the final rule in

73.54(a)(1)(ii) to specify security systems and networks, which include CAS and SAS cyber connections that are identified by site-specific analysis as requiring protection.

Comment Summary:
One commenter stated that the proposed rule requires the CAS and SAS be functionally equivalent, but cyber security requirements are not specified as one of the features that need to be equivalent.

NRC Response:
The NRC disagrees. The cyber security program requirements of this section apply to both CAS and SAS relative to security systems and networks. The final rule 73.55 requirement for functionally equivalent focuses on those functions that must be performed by either CAS or SAS during a contingency event.

Comment Summary:
One commenter suggested that there is no reason to delay implementing a comprehensive control system cyber security program. The commenter explained that the longer implementation is delayed, the longer nuclear power plants will be at risk.

NRC Response:
The NRC required through Commission Orders following the September 11, 2001, attacks that licensees take certain actions relative to digital computer and communication systems and networks. Therefore, there is no delay in implementing appropriate cyber security protection measures. This rulemaking establishes the regulatory framework for a cyber security program through which the licensee will provide protection against the DBT for cyber attacks consistent with 10 CFR 73.1 and incorporates lessons learned by the Commission through implementation of Commission Orders.

Comment Summary:
Two commenters stated that the proposed wording in 10 CFR 73.55(m)(1) does not allow for other compensating controls to satisfy the need for continued functionality. The commenters suggested that the NRC change the phrase “high assurance that computer systems” to “high assurance that the functionality provided by computer systems.”

NRC Response:
The NRC agrees in part. The NRC has revised the final rule to address continued functionality. However, the NRC determined that the requirements must focus on the prevention of adverse effects and the “integrity” of these systems and networks to perform their required functions *as intended*, as opposed to simply maintaining the ability to function. A compromised system or network can still “function” however, that functionality could cause harm as a direct or indirect result of the compromise, and therefore, the basis of these requirements are more appropriately focused on the integrity of these systems and networks to perform the required function as intended.

Comment Summary:
Two commenters indicated that the proposed rule language places cyber security within the licensees’ physical security organizations. One commenter explained that cyber security is not currently integrated into the site’s physical security organization. The other commenter suggested that the NRC put proposed 10 CFR 73.55(m) under proposed 10 CFR 73.58 or create a new rule for cyber security.

NRC Response:
The NRC's intent is that the cyber security program is incorporated and managed as part of the physical protection program but not necessarily implemented by physical security personnel. The NRC does not intend to dictate what personnel implement the cyber security program and recognizes that a unique technical expertise and knowledge is required to effectively implement the cyber security program as opposed to the physical protection program. As such, the NRC's expectation is that the personnel assigned to each program must be trained, qualified, and equipped to perform their unique duties and responsibilities. However, although the specific measures used may differ, both the physical and cyber security programs involve measures to detect, respond to, and neutralize threats within the design basis threat of radiological sabotage and, therefore, are intrinsically linked and must be integrated to satisfy the physical protection program design criteria of the final rule.

Therefore, the NRC agrees in part. The NRC agrees that the proposed 73.55(m) should be a stand-alone 10 CFR section. The NRC relocated the proposed 73.55(m) in its entirety to a new, stand-alone, 10 CFR section 10 CFR73.54 but retains the requirement that the cyber security program be a component of the physical protection program.

Comment Summary:
Another commenter endorsed the detailed NEI comments for this section and stated that he found agreement between NEI-04-04 and the proposed rule. However, the commenter noted that cyber security and its mitigation is not a physical security issue and should be relocated from the Safeguards Contingency Plan (SCP) because some of the detail is more appropriate for guidance documents.

NRC Response:
The NRC disagrees. 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 and therefore, must be integrated to satisfy the physical protection program design criteria of the final rule 10 CFR73.55(b).

Comment Summary:
Another commenter asked if “protected computer systems” are defined in the proposed rule, or if all computers onsite are affected by the cyber security rules. The commenter urged the NRC to be more specific in defining what a protected computer system is.

NRC Response:
The NRC agrees. The NRC has revised the final rule in 73.54(a)(1), to be more specific in defining what a protected computer system is. The term "protected computer systems" is replaced by the term "assets." The term "assets" is used to generically refer to the specific systems and networks that are identified by the licensee through site-specific analysis in 73.54(b)(1) as meeting the criteria in 73.54(a)(1).

Comment Summary:
One commenter questioned whether defense-in-depth in computer terms means real-time backup data. The commenter also questioned how this requirement impacts the video capture system, which is a computer system.

NRC Response:
The need to back up data, such as recorded video imagines, 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 protective strategies are technical and administrative controls that are used to mitigate consequences from a cyber attack. The final rule 73.55(b) requires that the physical protection program be designed to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT are maintained at all times. The licensee determines through a site specific analysis if recorded video imagines must be protected, and the measures needed to maintain these capabilities.

Comment Summary:
Two commenters stated that proposed 10 CFR73.55(m)(2) needs clarification. The commenters explained that licensees will assume that the assessment process defined in NEI 04-04, "Cyber Security Program for Power Reactors," will be sufficient to meet the rule requirements. However, the commenters believed NRC needs to include further clarification of what is meant by "assessment" to ensure that NEI 04-04 will meet the requirements. The commenters suggested that the NRC clarify this issue in the Statements of Consideration (SOCs).

NRC Response:
The NRC agrees that clarification is needed. The NRC revised the final rule (d)(2) to clarify that the cyber security program design must include a methodology to evaluate and manage cyber risks in a systematic manner in lieu of an independent assessment program. The intent of this requirement is to ensure that the measures used to protect digital computer and communication systems and networks are evaluated and managed in a manner that ensures they remain effective and continue to meet high assurance expectations.

Comment Summary:
Another commenter asked if the cyber security assessment program is intended to be real-time, during an initial assessment, or with periodic updates. If NRC wants periodic updates, the commenter asked what periodicity is required.

NRC Response:
Consistent with the requirements of the final rule, with regard to assessments and periodic re-assessments, licensees must evaluate changes to the cyber security posture when:
(1) modifications are proposed for previously assessed systems,
(2) new technology-related vulnerabilities not previously analyzed in the original baseline are identified and periodic assessments that would act to reduce the cyber security posture of the system are identified.
(3) there is a change in cyber threat or risk.

Comment Summary:
One commenter stated that the NRC should engage independent experts to develop a comprehensive computer vulnerability and cyber-attack threat assessment. The commenter explained that such an assessment must evaluate the vulnerability of the nuclear power plant's computer systems and the potential consequences.

NRC Response:
The NRC disagrees that independent experts are needed. It is the licensee's responsibility to

ensure that personnel assigned to evaluate and manage cyber risks are properly trained and possess the knowledge, skills, and abilities required to effectively perform this function. The results of the licensee's evaluation and management of cyber risks is subject to NRC inspection.

Comment Summary:
One commenter stated that the proposed language implies that much of the details of the cyber-security program will be classified as SGI. The commenter explained that this will place a large burden on the infrastructure of the cyber-security program. The commenter stated that the current designation of 10 CFR 10 CFR 2.390 should be adequate. The commenter also stated that having cyber security details in the Physical Security Plan (PSP), SCP, or Training and Qualification (T&Q) plan is not appropriate because cyber security is not a regulatory function for nuclear security organizations. The commenter recommended that cyber security requirements be relocated to a separate rule and implementing licensing document. If the NRC does not want to take this step, then the commenter suggested that the NRC clarify the details in the SOCs to state that cyber security program elements are not considered SGI.

NRC Response:
The NRC disagrees that approved security plans are by default considered SGI and stresses the fact that designation of any information as SGI is determined in accordance with the criteria set forth in 73.21. The determination of whether cyber security program related information must be protected is determined by the criteria established in 73.21. The NRC disagrees that cyber security is not a regulatory function for nuclear security organizations and has determined that because cyber attacks can adversely impact the ability of the licensee to protect against the design basis threat of radiological sabotage the cyber-security program is an important component of the overall physical protection program.

Comment Summary:
Another commenter explained that the summary of the cyber security program now contained in Chapter 18 of NEI 03-12, Revision 4 “Template for Security Plan and Training and Qualification Plan” (endorsed by the NRC) is sufficient to meet the requirement to maintaining a written cyber security plan. The commenter urged the NRC to include this clarification in the SOCs.

NRC Response:
The NRC agrees that current security plans address cyber security program requirements. However, the NRC disagrees that the approved plans are applicable to this rulemaking. The NRC has revised the final rule to require that each licensee document its cyber-security program in a stand-alone cyber-security plan in addition to the pre-existing Commission-approved physical security plan, safeguards contingency plan, and training and qualification plan.

Comment Summary:
One commenter urged the NRC to clarify that “Continuity of Power Systems” (as defined in NEI 04-04) when it refers to “maximize plant productivity” are outside the scope of this rule. The commenter explained that the NRC should include this clarification in the SOCs.

NRC Response:
The NRC agrees in part. The NRC agrees that the continuity of power systems for business systems used to produce electricity are outside the scope of this rulemaking and, as such, the NRC disagrees that topics ***not*** addressed herein should be identified in the SOCs.

Comment Summary:
One commenter stated 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. The commenter suggested that the NRC require licensees to demonstrate a plan of action to detect cyber attacks. The commenter also believed that the NRC should require licensees to change their current emergency call-out and response phone numbers and categorize the numbers as safeguarded data. The commenter suggested that the NRC receive third-party advice whenever a generic cyber-security upgrade is needed, rather than relying on a licensee's judgment. The commenter suggested the National Institute of Standards and Technology Computer Security Division as one advisory source.

NRC Response:
The NRC disagrees. This section establishes a performance-based requirement that would require timely detection of, and response to, a cyber security incident. Licensees are required to develop, implement, and maintain a plan of action to detect cyber attacks but are not required to meet deterministic time limits for discovery of a cyber attack. Depending upon the type of attack employed and the skill of the attacker, the results of the attack may not be immediately obvious (as in the case of 0-day attacks) or may require in-depth analysis to discount the possibility of false positives as reported by security monitoring systems. With respect to emergency call-out and response phone numbers, the criterion for determining information as SGI is contained in 10 CFR 73.21. Cyber security upgrades (whether generic or specific) are required to comply with the requirements of this section. The decision to use a third-party advice regarding upgrades resides with the licensee. The NRC agrees that NIST is one source of technical information, but does not dictate what information sources licensees should use.

Comment Summary:
One commenter stated that the incident response teams and plans should be tightly integrated with corporate plans. The commenter recommended that these plans remain outside Appendix C and be referenced in the onsite physical protection plan. To achieve this, the commenter recommended that the NRC require the cyber security incident response and recovery plan to be "summarized" and not "described" in the integrated response plan (IRP) required by Appendix C.

NRC Response:
The NRC agrees that the cyber security incident response and recovery plan is unique and can be appropriately addressed and maintained separate from the SCP described in Part 73 Appendix C, Section II. Therefore, the NRC has deleted this requirement from the final rule and consistent with the final rule 73.54(e)(2) requires that the incident response and recovery plan be addressed by the stand-alone "cyber security plan".

Comment Summary:
Another commenter stated that the cyber security incident response and recover plan does not belong in the Incident Response Plan (IRP) because the IRP outlines off-site law enforcement response to physical security events as defined in the SCP. Also, the commenter explained that if the cyber security response plan is placed in the SCP, much of the IRP would need to be exempt from SGI designation. Otherwise, the commenter stated, a great burden will be placed on the computer systems support organizations. The commenter suggested that the NRC delete this provision from the final rule.

NRC Response:

The NRC agrees in part. The NRC has deleted this requirement from the final rule and consistent with the final rule 73.54(e)(2) requires that the incident response and recovery plan be addressed by the stand-alone "cyber security plan".

Comment Summary:
Two commenters stated that the “considerations” for 10 CFR 73.55(m)(3)(i) refers to the “computer security program” as opposed to the “cyber security program.” The commenters urged the NRC to change “computer security” to “cyber security.”

NRC Response:
The NRC agrees. The NRC determined that this proposed requirement is sufficiently addressed by the final rule 73.54(f) and is, therefore, not necessary. The NRC has deleted this proposed requirement from the final rule.

Comment Summary:
One commenter stated that, in the wake of September 11, 2001, security at nuclear power plants should be increased the same way it is at airports and cargo terminals. The commenter stated that there should be a no fly zone and increased security from the air and water to make every attempt to prevent a terrorist attack.

NRC Response:
Following September 11, 2001, the physical protection programs implemented at nuclear power plants were significantly enhanced through a series of Commission Orders to account for the changing threat environment. This rulemaking reflects those enhancements. With respect to the specific programs required for airports, the requirements applied at power reactors are so significantly different that the two programs can not be equated. The pre-existing 10 CFR 73.55 requires similar search requirements for weapons and explosives that were applied as enhancements to airports after September 11, 2001. The final rule 73.55(e)(8)(ii) addresses water threats. The final rule 10 CFR 50.54(hh) addresses threats from aircraft. The Commission concluded that a requirement for no fly zones is beyond the scope of this rulemaking.

Comment Summary:
Another commenter stated that there are many references to “significant core damage” and “spent fuel sabotage,” but these phrases are sometimes linked by an “and” and sometimes by an “or.” The commenter stated that the two connectors can create very different results. The commenter noted that the two phrases are connected by “and” in 10 CFR10 CFR73.55(b)(3), (c)(1)(i),(f)(4), (g)(4)(ii)(C), (i)(4)(i), (k)(1)(i) and by “or” in 10 CFR10 CFR73.55(b)(7)(ii) and (t)(1)(ii).

NRC Response:
The Commission agrees and has revised final rule text to use the connector “and” consistently wherever the phrase significant core damage” and “spent fuel sabotage” is used.

Comment Summary:
The same commenter asked why the final section of proposed 10 CFR 73.55 is merely called “Definitions” and not given a more distinct reference, such as 10 CFR 73.55(u).

NRC Response:
The Commission has determined it is appropriate to define key terms in regulatory guidance and has revised this section accordingly.

Comment Summary:
Another commenter stated that the Power Reactor Security Requirements should fully address the potential consequences of the use of toxic chemicals or chemical weapons as part of an attack scenario. The commenter noted that there are many agents that are not only easy to make and transport, but do not require sophisticated methods to deploy.

NRC Response:

The final rule Appendix B, Section VI, requires that armed response team members be equipped with and trained to use, protective masks for protection against the use of chemical and biological weapons.

Comment Summary:
Another commenter stated that the term “unauthorized activities” is ambiguous and is not defined in 10 CFR 73.2. This term is used in the following sections: 10 CFR 73.55(d)(4); (d)(5); (e)(5)(i)(B); (e)(5)(ii); (e)(6)(vi); (e)(8)(vi); (e)(9)(iii); (g)(1)(vi); (h)(5); (h)(7); (i)(4)(i); (i)](6); (i)(8)(iv); (i)(9)(i); (i)(9)(ii); (i)(9)(v); (i)(10)(ii)(B); (l)(4)(iii); (l)(4)(v)(C); and (m)(5).

NRC Response:
The Commission agrees in part. The Commission has determined that the word “unauthorized” is retained from the pre-existing 73.55(c)(4). The word “unauthorized” as used in the proposed rule was intended to be generic and site-specific. Nonetheless, the Commission has deleted the term "unauthorized activities" from the final rule.

Comment Summary:
One commenter stated that proposed 10 CFR 73.55(d)(1), (e), (g)(1)(i), (g)(2), (g)(3), (h), and (i)(1) appear to impose new requirements to the Owner Controlled Area (OCA) that previously only applied to the protected area (PA) (e.g., barriers, intrusion detection, search, etc.). The commenter argued that results of the NRC Force-on-Force inspections do not support expanding these requirements beyond the PA.

NRC Response:
The Commission agrees in part. The NRC has revised the final rule to clarify that physical protection measures applied inside the OCA are determined on a site-by-site basis through site-specific analysis as needed to satisfy the physical protection program design requirements of 10 CFR 73.55(b). The final rule requires that each licensee identify and account for site-specific conditions that necessitate the use of physical barriers in the OCA. The Commission's expectation is that each licensee will implement security measures in the OCA as needed to ensure the physical protection program is effective.

Comment Summary:
Regarding proposed 10 CFR 73.55(a)(1), one commenter, supported by another commenter, stated that once the final rule and detailed supporting guidance is published, NEI 03-12 will require revision. The commenter said a significant amount of time is then necessary to review the guidance, prepare the necessary changes to NEI 03-12, and submit NEI 03-12 to NRC for endorsement. Once endorsed, the commenter said the licensee will prepare their individual plan changes and submit them to the NRC for approval. The commenter argued that, given this level of effort, the 180 days does not appear to be workable. The commenter said the rule language must consider the amount of time involved in completing these tasks. The other commenter recommended that the NRC change the effective date to 180 days after NRC’s endorsement of the revised NEI 03-12.

NRC Response:
The NRC agrees in part. Upon review, the Commission determined that the majority of the amended requirements of this rulemaking are already captured in the current NRC-approved security plans as a result of the October 2006, Commission approval of revised security plans. Consistent with this approval, the Commission further concluded that an additional review and

approval of these pre-existing security plans is not necessary, except as needed to address the new requirements of this section and the new Cyber Security Plan required by the final rule in 10 CFR 73.54. As a result, the Commission has revised the final rule to require licensees to make appropriate plan changes in accordance with 10 CFR 50.54(p), 50.90 and 73.5. Consequently, the Commission determined that 180 days is sufficient time for licensees to identify their site-specific needs and make appropriate changes to the approved plans.

Comment Summary:
One commenter asked how much time would be given to licensees to revise their security plans, and whether they must submit the plans under the provisions of 10 CFR 50.90 and 10 CFR 50.54.

NRC Response:
As stated above, licensees are given 180 days to identify site-specific needs and to make appropriate changes to the site security plans.

Comment Summary:
Another commenter asked whether, under the new rule, the licensees' new plans will be subject to approval by the NRC.

NRC Response:
As stated above, the Commission determined that review and approval of the pre-existing security plans is not necessary, except as needed to address the new requirements of this section and the new Cyber Security Plan required by the final rule in 10 CFR 73.54.

Comment Summary:
One commenter stated that proposed 10 CFR 73.55(a)(2) would require the security plans to include a description of how the revised requirements will be implemented by the licensee, and a proposed implementation schedule. The commenter said this information is not appropriate to be placed in the security plan. Thus, the commenter recommended that the NRC revise 10 CFR 73.55(a)(2) in the final rule by deleting "and must describe how the revised requirements of this section will be implemented by the licensee, to include a proposed implementation schedule."

Also, the commenter stated that, in accordance with 10 CFR 73.55(a)(1), the security plans must contain the proposed revised requirements, thus the 10 CFR 73.55(a)(2) requirement to include descriptions is redundant. Also, the new security plans will become effective upon NRC approval. Therefore, the commenter stated that the 10 CFR 73.55(a)(2) requirement to include a proposed implementation schedule is not applicable.

NRC Response:
The Commission disagrees. It is appropriate for security plans to describe how Commission requirements will be implemented and the final rule, in 10 CFR 73.55(a)(2) and (c)(1)(i) explicitly requires such a description. The required description is necessary to determine the general compliance of each licensee with NRC requirements. The final rule 10 CFR 73.55(a)(2) is revised consistent with the determination that revised plans (in their entirety) are not necessary.

Comment Summary:
In reference to proposed 10 CFR 73.55(a)(4), 73.55(c)(1), and 73.55(t)(2), one commenter noted that "the first reference states that licensees will implement the physical protection

program in accordance with Commission regulations, etc., and the second reference appears to support that. However, the second reference acknowledges that alternative measures could be submitted in accordance with 10 CFR 50.4 and 50.90 and, therefore, might be approved by the Commission." The commenter asked: "What is the legally controlling document, the regulations or the licensees' NRC-approved physical security plans?"

NRC Response:
The Commission concluded that this comment may reflect an over simplification of the NRC regulatory processes. It is more accurate to state that both the NRC's regulations and the NRC-approved plans are legally controlling, however, the fact that a licensee has an NRC-approved security plan does not relieve the licensee from compliance with NRC regulations. NRC regulations are legally controlling in that they set forth the regulatory framework and general performance objectives and requirements to be implemented by each licensee. The NRC-approved plans describe how the licensee will comply with NRC regulations through implementation, which ***includes*** any NRC-approved exemptions and alternatives. To the extent that there are differences between the licensee's security plan and NRC requirements, those differences must be explicitly approved by the NRC, through an NRC-granted exemption (10 CFR 73.5), or an NRC-approved "alternative measure" (final rule 10 CFR 73.55(r)).

The Commission recognizes that generic regulations cannot always account for site-specific conditions and, therefore, has determined that some degree of regulatory flexibility is necessary to ensure that each licensee is able to design their physical protection program to effectively satisfy the "high assurance" performance objective in the final rule (10 CFR 73.55(b)). Therefore, the final rule is revised to address the mechanisms through which the Commission reviews and approves a licensee's need for an alternative measure or exemption from one or more NRC requirements provided sufficient justification is demonstrated.

Upon the NRC's written approval, the measure or measures specified by the NRC in writing, become legally binding as a license condition in lieu of the specific requirement stated in the regulations. It is important to note that the fact that the NRC may have approved a security plan containing a deficiency or conflict, does ***not*** shield the licensee from regulatory compliance. In such cases the NRC and licensee will work together to resolve the conflict and if needed, changes could be made to the licensee's security plans to ensure all Commission requirements are met.

Comment Summary:
Another commenter stated that in proposed 10 CFR 73.55(a)(4) the word "related" is ambiguous. The commenter stated that proposed 10 CFR 73.55(a)(4) would lead one to believe that compliance with all "site implementing procedures" would be required by the Rule, but there are many site and security procedures not committed to in the security plans. The commenter recommended that the NRC modify this section by deleting "related" and "and site implementing procedures".

NRC Response:
The Commission agrees. The Commission deleted the term "related" in this section of the final rule.

Comment Summary:
The terms "significant core damage" and "spent fuel sabotage" should be replaced with the term "radiological sabotage" because "radiological sabotage" is a defined term in 10 CFR 73.2 and

the other terms are not.

NRC Response:
The Commission disagrees. The Commission has added 10 CFR 73.55(b)(2) to clarify that the pre-existing requirement in 10 CFR 73.55(a) to "protect against the DBT of radiological sabotage" is retained without modification. "Significant core damage" and "spent fuel sabotage" are design requirements for the physical protection program. As used, the terms "significant core damage" and "spent fuel sabotage" are consistent with the use of these terms prior to and after September 11, 2001. The proposed 73.55(b)(2) has been renumbered in the final rule to 10 CFR 73.55(b)(3).

Comment Summary:
The proposed rule language is too detailed, prescriptive, and not performance based. This level of detail is inappropriate for inclusion in rule language. It is appropriate for inclusion in guidance.

NRC Response:
The Commission disagrees. Performance-based rules must contain measurable performance-criteria and the Commission has concluded that the capability to protect the public health and safety against the design basis threat of radiological sabotage is directly dependent on the capability to prevent significant core damage and spent fuel sabotage, which is a direct result of the licensee capability to protect target sets.

Comment Summary:
The proposed language and statements of consideration do nothing to change the definition of radiological sabotage. If the concern is truly with the definition of radiological sabotage, then it should be revised. It is not clear how the definition of "radiological sabotage" stated in 10 CFR 73.2 contains a performance based element by which the Commission can measure is addressed.

NRC Response:
The Commission agrees in part. The Commission agrees that the proposed rule and statements of consideration do nothing to change the definition of radiological sabotage nor does the NRC intend, or believe, that there is a need to revise this definition. As stated in 10 CFR 73.2, radiological sabotage means "Any deliberate act..." and, as such, this definition is excessively broad and can not be measured.

The Commission revised the final rule to clarify that, although the pre-existing requirement for protection against radiological sabotage is retained without modification, the focus of the physical protection program *design* must be on preventing significant core damage and spent fuel sabotage through the protection of target sets against the DBT. As such, the Commission has concluded that significant core damage and spent fuel sabotage is the appropriate performance-criteria against by which the licensee's capability to protect against radiological sabotage can be measured.

Comment Summary:
A literal reading of the rule language is that a physical protection program is not capable of protecting against radiological sabotage unless it has six specific elements. All six elements are not required to protect against acts of radiological sabotage.

NRC Response:
The Commission agrees in part. The Commission has revised the final rule to use the term "interdict" in lieu of the three terms "intercept, challenge, and delay." The Commission concluded that the term interdict more concisely represents Commission expectations. The Commission agrees that a physical protection program is not effective unless it has all four elements and disagrees that all four elements are not required to protect against radiological sabotage. To be effective a physical protection program must possess and maintain the ability to ***detect*** the presence of a threat, ***assess*** the threat capabilities to determine appropriate response, ***interdict*** a response between the threat and the protected items before the threat reaches its objective or target, and ***neutralize*** the capability of the threat to cause harm or otherwise complete its objective.

Therefore, a physical protection program is ***not*** capable of protecting against radiological sabotage unless it meets these four (4) performance-criteria. A failure of any one element could result in a failure of the program to protect the public health and safety against radiological sabotage.

Comment Summary:
The proposed language and discussion in the statement of considerations is confusing and inconsistent. The statement of considerations references the existing regulatory requirement which is delineated in 10 CFR 73.55(a) and notes it is being revised to provide a more detailed and performance based requirement for the design of the physical protection program. However, the statement of considerations also cites the existing 10 CFR73.55(h)(4)(iii)(A) as the section with language that is problematic. So, which of the existing regulations are intended to be modified?

NRC Response:
This requirement is not intended to modify either current requirement but rather, retains and combines the current requirements of 10 CFR73.55(a) to protect against the Design Basis Threat (DBT), and 10 CFR73.55(h)(4)(iii)(A) to interpose. The Commission's intent is to clarify that both requirements are directly related and address critical physical protection program design features. To protect against and interpose the DBT, the licensee must detect and assess the threat and then interdict and neutralize that threat. Therefore, the four terms detect, assess, interdict, and neutralize are appropriate performance-criteria to be met.

Comment Summary:
10 CFR 73.55(h)(4)(iii)(A) is modified later in the proposed rule in section 73.55 (K)(7)(iii). The language in that section cites four of the six criteria delineated in (b)(2) yet those six criteria are intended to address the concern with the word “interpose” which only appears in 10 CFR73.55(h)(4)(iii)(A). The linkage between the language in 10 CFR73.55(h)(4)(iii)(A) and in (b)(2) not clear and should be explained and justified.

NRC Response:
The revised 73.55(k)(7)(iii) focuses on the action “interpose”, which is represented in the final rule text as "interdict and neutralize". Because 73.55(k)(7)(iii) focuses only on the action "interpose", the two design features “detect and assess” are not addressed as these two actions would have already been completed in order to reach the action "interpose".

Comment Summary:
Further, these six elements do not apply to all threat conditions. For example, defense against

a large vehicle bomb is not likely to require all six capabilities.

NRC Response:
The Commission agrees. The fact that any one of the six performance-criteria (revised to four) does not apply to any one scenario does not invalidate its applicability. The Commission agrees that not all four performance-criteria apply equally in all possible scenarios. However, any one scenario will always contain at least one or more of the four performance-criteria and, therefore, each one is a valid design requirement by itself.

For example, the function of a Vehicle Barrier can interdict and/or neutralize a vehicle bomb without detection and assessment. However, it is the Commission's expectation that the physical protection program is not limited to only protection against vehicle bombs but also includes all other threats up to the full DBT to include a ground assault, and therefore, the detect and assess performance-criteria as well as the interdict and neutralize performance-criteria apply to scenarios involving the DBT adversary force.

Comment Summary:
In a performance based environment, performance assessments properly focus on outcomes not the underlying processes.

NRC Response:
The Commission agrees that a performance-based rule must focus on “outcomes” and the Commission's expectation is that the licensee's physical protection program design will focus on the elements needed to detect, assess, interdict, and neutralize the DBT before significant core damage and spent fuel sabotage is completed and, therefore, provide the *outcome* of high assurance that the public health and safety is protected against radiological sabotage.

Comment Summary:
The language in the rule is not consistent with the order language in regards to “single act” and appears to expand the requirement beyond what was required by the order (reference Section 3 of the April 29, 2003 DBT Order). The commenter recommended that 10 CFR 73.55(b)(3) be revised as follows: (b)(3) The licensee physical protection program must be designed and implemented to satisfy the requirements of this section and ensure that no single act, as bounded by the design basis threat, can ~~disable the personnel, equipment, or systems necessary to prevent significant core damage and spent fuel sabotage~~ result in radiological sabotage. The terms “significant core damage” and “spent fuel sabotage” should be replaced with the term “radiological sabotage” because “radiological sabotage” is a defined term in 10 CFR 73.2 and the other terms are not. The rule should include a definition of “no single act.”

NRC Response:
The Commission agrees in part. The Commission agrees that the proposed requirement intended to expand the pre-existing requirement for protection against a single act, and disagrees that the proposed requirement was not consistent with Commission Orders. Nonetheless, the Commission concluded that the term "single act" is specific to the Central Alarm Station/Secondary Alarm Station (CAS/SAS) survivability and functionality, and that protection of personnel, systems, and equipment is specific to protection against the vehicle bomb attributed to the DBT. This requirement intended to consolidate the protection of personnel, equipment, and systems against a vehicle bomb with the pre-existing requirement for protection of CAS/SAS against a single act into one performance-based requirement.

Upon review the Commission concluded that it is more appropriate to address each requirement individually and has revised the final rule 10 CFR 73.55(i)(4)(i) to address “single act” and the final rule 10 CFR 73.55(e)(10)(i)(A) to address protection of personnel, systems, and equipment. The Commission’s expectation is that each licensee will ensure survivability of either CAS or SAS against a single act within the DBT capabilities and will protect personnel, systems, and equipment required to maintain safe shutdown capability, and implement the protective strategy, against a vehicle bomb.

Comment Summary:
The scope of the statement in 10 CFR 73.55(b)(4) is far reaching and ambiguous. As written, this requirement appears to impose more stringent design criteria than for safety-related systems. The language used in (b)(4) does not match the SOC discussion. The focus of the SOC is on defense in depth which is currently described in NEI 03-12. At the March 9, public meeting (see Page 23 of the meeting transcript) the NRC clarified that the intent of this new requirement was not to produce a completely diverse and redundant system for every attribute of the site security plan. Given the clarification on this provision the commenter recommended revising 10 CFR 73.55(b)(4) as follows: “(b)(4) The physical protection program must include defense in depth. ~~diverse and redundant equipment, systems, technology, programs, supporting processes, and implementing procedures.~~ “

NRC Response:
The Commission agrees in part. The Commission has revised the final rule to use the phrase "defense-in-depth". The proposed rule and the SOCs attempted to describe defense-in-depth with performance-based language consistent with how this long-standing and professionally accepted standard is applied. Defense-in-depth begins with security measures in the OCA (least stringent) and includes progressively more stringent measures through the Protected Area (PA) to Vital Areas (VAs). Defense-in-depth ensures that the failure or bypass of any one component of the physical protection program does not cause a failure of the entire program. In the case of equipment failure, compensatory measures are commonly used to ensure that the function performed by the failed equipment is maintained and could involve back-up equipment or personnel.

Comment Summary:
A commenter recommended deleting 10 CFR 73.55 because he believed that it is redundant to the requirements specified in Appendix B and C to this part. If retained, the commenter recommended that it be revised as follows: “(b)(6) The licensee shall establish and maintain a ~~written~~ performance evaluation program in accordance with appendix B and appendix C to this part, to demonstrate and assess the effectiveness of armed responders and armed security officers to perform their assigned duties and responsibilities to protect target sets described in paragraph (f) of this section and appendix C to this part, through implementation of the licensee protective strategy.”

NRC Response:
The Commission agrees in part. This requirement is necessary to establish the regulatory framework for the requirements in Appendix B. The Commission agrees that the performance evaluation program need not be a completely independent written program and has revised the final rule to require that this program be documented to provide flexibility and allow the licensee to utilize existing documentation to represent this program.

Comment Summary:
In 10 CFR 73.55(b)(8), replace the word “Measures” with the words “The program”. It is the corrective action program that must ensure necessary and appropriate actions are initiated.

NRC Response:
The Commission agrees. The Commission has revised final rule text to incorporate the requested change and other clarifying revisions.

Comment Summary:
A commenter stated that the Commission should change the broad definition of “Security plans” to embrace all the plans that are included in it (i.e., “physical security plan,” “training and qualification plan,” and “safeguards contingency plan”). The commenter stated that a possible solution is to simply name the section “Plans”.

NRC Response:
The Commission agrees in part. Consistent with the 10 CFR 73.55(a) introduction, the four plan titles are consolidated under the generic title “security plans”. The Commission has determined that the term “security” is commonly understood by both industry and the public to be the focus of these plans and is needed to prevent confusion with other site plans.

Comment Summary:
One commenter stated that it is logical that power plants situated near highly populated metropolitan areas are more likely to be selected as targets, so the PRSRs should be modified to require a customized approach to security at high target nuclear facilities.

NRC Response:
The Commission agrees in part. The Commission agrees that a customized approach to security is necessary at all sites. The Commission requires in 10 CFR 73.55(b)(4) that licensees analyze their site-specific conditions in the design of the physical protection program.

Comment Summary:
Another commenter noted that proposed 10 CFR 73.55(c)(3)(ii) may imply that the details of a cyber-security plan will be classified as Safeguards Information (SGI). The commenter stated that this would greatly extend the timeframe and complicates the implementation of a cyber-security program. The commenter recommended that the Commission clarify the SOCs to state that some elements of the physical security plan (PSP) may not be SGI even though the PSP itself is controlled as SGI (e.g., cyber security requirements).

NRC Response:
Compliance with this provision requires that each licensee review each security plan in accordance with the criteria established in 10 CFR 73.21 and portion mark the security plans appropriately.

Comment Summary:
A commenter stated that proposed 10 CFR 73.55(c)(2) is redundant to the requirements in 10 CFR 50.34(e) and 73.21. As such, and since 10 CFR 73.55 licensees must comply with 10 CFR 50.34(e) and 73.21, the commenter argued that this redundant rule is unnecessary. In addition, the commenter noted that the reference to 10 CFR 73.21 will soon need to be change to 10 CFR 73.22 and 10 CFR 73.23 upon issuance of the proposed SGI rules. The commenter stated that proposed 10 CFR 73.22 and 10 CFR 73.23 basically state the same as the current

10 CFR 73.21 with some wording changes. Thus, the commenter recommended that the Commission delete 10 CFR 73.55(c)(2) from the final rule, as it is redundant to the current 10 CFR 50.34(e) and 73.21 and serves no purpose.

NRC Response:
The Commission disagrees. This requirement is necessary to clearly identify handling and protection requirements for security plans in this regulatory framework. In addition, the Commission disagrees that reference to 10 CFR 73.21 will necessitate future changes to this rule text. The Commission understands that 10 CFR 73.22 and 73.23 may be added, but that 10 CFR 73.21 will remain as the primary regulatory text through which 10 CFR 73.22 and 73.23 will be linked, and therefore, reference to 10 CFR 73.21 in this rule text establishes the necessary regulatory link to all three.

Comment Summary:
One commenter noted that proposed 10 CFR 73.55(c)(3)(i) is redundant with 10 CFR 50.34(c) and each licensee's License Conditions. Thus, the commenter recommended that the Commission delete this section from the final rule.

NRC Response:
The Commission disagrees. The Commission has determined that this requirement is necessary to establish the regulatory framework for the physical security plan in this section.

Comment Summary:
One commenter stated that the Commission should incorporate the proposed rule wording in the new 10 CFR 73.55(c)(4)(ii) into 10 CFR 50.34 to be consistent with existing 10 CFR 50.34(c) and (d). The commenter also recommended that the Commission delete proposed 10 CFR 73.55(c)(4)(ii) and integrate it into a new 10 CFR 50.34 (e) to be consistent with 10 CFR 50.34(c) and (d).

NRC Response:
The Commission agrees in part. The current requirement for a Training and Qualification Plan is found in 10 CFR 73.55(b)(4)(ii) and not 10 CFR 50.34. The Commission has made conforming changes to 50.34(c) to require both the cyber security plan and the training and qualification plan as part of the physical security plan. The Commission retains this requirement in the final rule to consolidate and describe the requirements for all four required plans in one 10 CFR location.

Comment Summary:
The same commenter stated that proposed 10 CFR 73.55(c)(4)(ii) could be interpreted as requiring all members of the security organization to have training requirements equivalent to those for the uniformed security organization. Thus, the commenter recommended that the Commission revise 10 CFR 73.55(c)(4)(ii) in the final rule to state: "The training and qualification plan must describe the process by which armed and unarmed security personnel, *and* watchpersons will be selected, trained, equipped, tested, qualified, and re-qualified to ensure that these individuals possess and maintain the knowledge, skills, and abilities required to carry out their assigned *security duties effectively in accordance with appendix B, General Criteria for Security Personnel*."

NRC Response:
The Commission agrees in part. This requirement has been determined to be redundant to the

final rule Appendix B, Section VI, and is deleted from this section. The Commission agrees that administrative staff such as secretaries, file clerks, and cyber security staff would not require Appendix B type training equal to uniformed personnel, however, the Commission *does* intend to require task-specific training of *facility personnel*, uniformed or not, who are assigned duties and responsibilities associated with implementation of the physical protection program. Specifically, the Commission intends to include facility personnel performing duties such as, vehicle escorts, searches, and/or compensatory measures for failed security equipment or systems.

Comment Summary:
One commenter stated that the proposed rule wording in 10 CFR 73.55(c)(5)(i) is redundant to the requirements specified in 10 CFR 50.34(d) and each licensee's License Condition. The commenter recommended that the Commission delete this provision as it is redundant to existing 10 CFR part 50 rule requirements and license conditions for nuclear facilities.

NRC Response:

The Commission disagrees. The Commission has determined that this requirement is necessary to establish the regulatory framework for the safeguards contingency plan in this section.

Comment Summary:
One commenter noted that draft final Part 52 rule includes requirements for design certification applicants to include a description and evaluation of the design features or strategies for the prevention and mitigation of a specific set of severe accidents. The commenter acknowledged that action should be taken to prevent or mitigate certain specific beyond design bases events including those resulting from large fires and explosions. To improve regulatory coherency and consistency, the commenter stated that the Commission should address large fires and explosions in the same regulation and in the same manner as other similar beyond design bases events that are already being addressed in the regulations. The commenter noted that the evaluations of the features and strategies that could mitigate or prevent beyond design bases accidents that result from large fires and explosions are performed by engineering and operational groups and NRC reviews are performed by engineering and operations inspectors. Therefore, the commenter stated that it is more appropriate for these matters to be addressed in Part 52 as opposed to Part 73.

NRC Response:
The Commission agrees. The Commission has determined that this comment more accurately addresses the proposed requirements in Appendix C, Section II., paragraphs (j) and (k)(1). The NRC has revised final rule text to move these requirements from the proposed Appendix C to a new 10 CFR 50.54(hh) because the specific requirements associated with this topic are currently implemented through "license conditions".

Comment Summary:
One commenter stated that the proposed language is too detailed, prescriptive, and not performance-based. The commenter argued that this level of detail is inappropriate for inclusion in rule language, but is appropriate for inclusion in guidance. The commenter suggested that the rule language be modified to state that "the safeguards contingency plan must describe predetermined actions, plans, and strategies designed to protect against threats up to and including the design basis threat of radiological sabotage."

NRC Response:
The NRC agrees in part. The NRC has revised final rule text in 10 CFR 73.55(c)(5) to generically address the contents of the Contingency Plan and has deleted this requirement because it is redundant to the specific requirements in Appendix C, Section II.

Comment Summary:
Another commenter noted that proposed 10 CFR 73.55(c)(5)(ii) specifies that the safeguards contingency plan (SCP) "must describe predetermined actions" for threats "up to and including the design basis threat of radiological sabotage." The commenter stated that this language is problematic because there is no cutoff in planning for minor events that do not pose a threat of radiological sabotage. The commenter argued that there is no need for the rule to be open-ended regarding the scope of contingency planning, and predetermined actions for lesser events can adequately be addressed in the NRC endorsed industry template for the SCP. Therefore, the commenter suggested that the Commission delete the phrase "threats up to and including" so that the section reads "The safeguards contingency plan must describe predetermined actions, plans, and strategies designed to intercept, challenge, delay, and neutralize the design basis threat of radiological sabotage."

NRC Response:
The Commission disagrees. The Commission has determined that the pre-existing scope for contingency planning and predetermined actions includes threats that do not constitute the full DBT, such as a civil disturbance. The Commission disagrees that there is no need for the rule to include such lesser events because such lesser events have the potential to escalate and therefore, must also be reconciled. The Commission has determined that the phrase "up to and including" is appropriate and necessary to clearly identify that the licensee must protect against all the capabilities of the DBT.

Comment Summary:
Another commenter stated that industry understands that the summary of the cyber security program now contained in Chapter 18 of NEI 03-12, Revision 4 "Template for Security Plan and Training and Qualification Plan" is sufficient to meet the proposed 10 CFR 73.55(c)(3)(i) requirement. The commenter noted that NEI 03-12 Revision 4 has been endorsed by the NRC, and this clarification should be provided in the SOC.

NRC Response:
The Commission disagrees. While the NRC has endorsed certain documents currently used by industry, the requirements for the cyber security program at power reactors are contained in the new 10 CFR 73.54. Acceptable methods of meeting these requirements are provided in draft regulatory guidance. The purpose of the SOC for this rulemaking is to provide clarifying information relative to Commission intent and expectations for these requirements and is not intended to provide endorsement of industry documentation.

Comment Summary:
One commenter stated that to incorporate the level of detail delineated (i.e., specific actions) will require an extensive re-write of existing site procedures. The commenter argued that many of the decisions and most of the actions cannot be forethought and cannot be documented in implementing procedures. Further, the commenter noted that the specificity of the requirement prevents the licensee from being able to provide the necessary flexibility to each member of the security organization to respond to the infinite spectrum of threats. Therefore, the commenter suggested that the NRC delete the word "specific" from 10 CFR 73.55(c)(6)(iii).

NRC Response:
The Commission agrees. Upon review, the Commission has determined that the use of the term "specific" is too extensive and not appropriate. Implementing procedures, by their very nature, must account for site-specific conditions and are subject to change. As such, implementing procedures must generally describe how each individual should respond in certain situations and conditions consistent with the effective implementation of Commission requirements. Therefore, the Commission has revised the final rule by replacing the word "specific" with the phrase "types of" to avoid unnecessary regulatory burden.

Comment Summary:
One commenter noted that the proposed rule language for 10 CFR 73.55(c)(6)(iv)(C) is noted in the SOCs as being new, but the impacts are not evaluated in the Regulatory Analysis. The commenter stated that the security organization is not equipped to review all site procedures every time a security procedure is modified. The commenter argued that implementation of this proposed requirement, as written, will have a significant impact on the organization and require additional security resources with the appropriate knowledge of all site procedures.

The commenter noted that at the March 9, 2007, public meeting the NRC clarified the intent of this section as applying to only security procedures and it is not the intent of this section to get into operational areas. Given this clarification, the commenter recommended that the Commission delete this provision from the proposed rule, as it is redundant to proposed 10 CFR 73.58. If retained, the commenter recommended the following revision to the provision: "Ensure that changes made to security implementing procedures do not decrease the effectiveness of any procedure to implement and satisfy Commission security requirements".

NRC Response:
The Commission agrees in part. The Commission disagrees that the proposed rule SOCs identify this requirement as new. The proposed SOCs state that this requirement is added to update and clarify the current regulatory framework. The current 10 CFR 73.55(b)(1)(i) requires licensees to comply with NRC requirements and the approved security plans, and 10 CFR 73.55(b)(3) requires a management system for controlling security procedures. As procedures implement security plans and plans implement requirements, the licensee must ensure that changes to procedures do not conflict with NRC requirements. The Commission agrees that the review of non-security procedures would have significant unintended impact and has revised the final rule to clarify that this requirement is limited to physical protection program implementing procedures. Given this clarification, the Commission disagrees that this requirement is redundant to 10 CFR 73.58 and has retained it.

Comment Summary:
Similarly, another commenter stated that proposed 10 CFR 73.55(c)(6)(iv)(C) is vague, open-ended, and appears to require all site "implementing procedures" to be reviewed to detect any decrease in effectiveness in satisfying any Commission requirement. The commenter suggested that this provision should be reworded to be consistent with the Commission approved SCP requirements. Therefore, the commenter suggested that the NRC modify the provision to be consistent with SCP, Section 3.3, as follows: "Ensure that changes made to facility implementing procedures required to effectively implement the site's protective strategy do not decrease the physical security effectiveness."

NRC Response:
The Commission agrees in part. The Commission agrees that the review of non-security

procedures would have significant unintended impact and has revised the final rule to clarify that this requirement is limited to physical protection program implementing procedures. Given this clarification, the Commission disagrees with the suggested rule text change.

Comment Summary:
A third commenter stated that 10 CFR 73.55(c)(6)(iv)(C) imposes on licensee procedures the same requirement that is currently only imposed on approved security plans. While the commenter admits that this is wise, the requirement imposes a similar standard for something that is not NRC-approved as that which is required for something that is NRC-approved.

NRC Response:
The Commission agrees in part. The Commission has revised the final rule to clarify that this requirement is limited to physical protection program implementing procedures. This proposed requirement used similar language as that of 10 CFR 50.54(p) to clarify the pre-existing 10 CFR 73.55(b)(1)(i) and 73.55(b)(3). Upon review, the Commission has also revised the final rule to clarify that changes must be reviewed to ensure continued compliance with NRC requirements rather than a subjective "decrease" of effectiveness.

Comment Summary:
In 10 CFR 73.55(d)(1), one commenter stated that the terms “early detection” and “unauthorized activities” are not defined and can have many different connotations resulting in significant impact on current programs. Also, the commenter stated that this provision does not match up with the performance criteria from proposed 10 CFR 73.55(b). The commenter noted that the term “any area” is nonspecific and can be interpreted broadly and that licensees only need monitor those areas necessary to successfully implement the physical protection program.

Therefore, the commenter recommended that the Commission eliminate the qualifiers “early,” “unauthorized activities,” and “any area” from the provision and reword it to state: “The licensee shall establish and maintain a security organization designed, staffed, trained, and equipped to provide detection, assessment, and response to protect the facility against radiological sabotage.

NRC Response:
The Commission agrees in part. The Commission has revised the final rule to clarify design requirements for the licensee security organization. The focus of this requirement is on an effective physical protection program that has the capability to detect, assess, interdict, and neutralize the design basis threat of radiological sabotage relative to preventing significant core damage and spent fuel sabotage. The Commission expectation is that the licensee will provide appropriate protective measures in any facility area for which site-specific analysis has determined that protective measures are needed. The licensee determines, subject to NRC inspection, the areas for which physical protection measures are needed consistent with its protective strategy.

Comment Summary:
A third commenter stated that the proposed phrase “within any area of the facility” in 10 CFR 73.55(d)(1) could be interpreted to include the OCA, PA, and VA, which would have the potential to drive early detection, assessment, and response beyond the area currently covered. The commenter noted that the SOCs describe the identification of a threat before an attempt to penetrate the PA. This is consistent throughout the proposed rule and drives each site to

protect an area that was previously viewed only as a licensee-owned “buffer zone.”

The commenter argued that the expectation to detect, assess, and respond for any area of the facility is unnecessary to demonstrate an effective defensive strategy and cannot be implemented due to the layout and geography at many sites. Therefore, the commenter suggested that the Commission should delete this new requirement and reword proposed 10 CFR 73.55(d)(1) as follows: “The licensee shall establish and maintain a security organization designed, staffed, trained, and equipped to provide detection, assessment, and/or response to unauthorized activities within the facility owner-controlled area as described in the Commission-approved security plans”.

NRC Response:
The Commission agrees in part. The Commission has revised the final rule to clarify design requirements for the licensee security organization. The focus of this requirement is on an effective physical protection program that has the capability to detect, assess, interdict, and neutralize the design basis threat of radiological sabotage relative to preventing significant core damage and spent fuel sabotage. The Commission expectation is that the licensee will provide appropriate protective measures in any facility area for which site-specific analysis has determined that protective measures are needed. The licensee determines, subject to NRC inspection, the areas for which physical protection measures are needed consistent with its protective strategy..

Comment Summary:
Another commenter stated that requiring the licensee to detect, assess, and respond to unauthorized activities in “any area of the facility” is too broad and goes beyond the legislative intent of the Atomic Energy Act by requiring the licensee to protect even the non-radiological areas of the plant. The commenter explained that “any area” of the plant could include training facilities, administration buildings, and equipment sheds, for which “unauthorized activities” would be quite different from those within the operational areas of the plant itself.

NRC Response:
The Commission disagrees that such areas are beyond the legislative intent of the Atomic Energy Act. The Commission has determined that the physical protection program must provide protection against the DBT in any facility area provided the DBT could disable the personnel, systems, or equipment required to prevent significant core damage and spent fuel sabotage from that area. The licensee determines, subject to NRC inspection, the areas for which physical protection measures are needed consistent with its protective strategy.

Comment Summary:
Another commenter stated that if there was ever a major incident at a nuclear power reactor, the license should not be renewed. The commenter clarified that if the license is renewed, there should be a requirement for increased safety staffing and procedures to make every effort to avoid an accident.

NRC Response:
The NRC has determined that this comment is not within the scope of this rulemaking.

Comment Summary:
One commenter stated that 10 CFR 73.55(d)(3) could be interpreted as requiring training and

qualification (T&Q) training for any “member of the security organization.” Therefore, the commenter suggested that the Commission replace the phrase “member of the security organization” with the phrase “an armed responder, armed security officer, alarm station operator, or watchperson”.

NRC Response:
The Commission disagrees. The Commission intends to include unarmed individuals, and non-security organization facility personnel, who perform security program duties and responsibilities such as escort duties, compensatory measures, and search functions. The Commission has revised the final rule to clarify that all personnel implementing the physical security program must be trained and qualified to the level of training and qualifications necessary to effectively perform their specific duties.

Comment Summary:
Two commenters referenced proposed 10 CFR 73.55(d)(5)(ii). One commenter asked: What is the difference between this provision and 10 CFR 73.55(r)(1)? If they are the same, the commenter suggested that the NRC delete one of the requirements to avoid confusion over purpose and scope.

NRC Response:
The Commission agrees. The Commission has deleted this paragraph but retains this requirement in 10 CFR 73.55(q)(1) "Records". This requirement focused on conditions to be specified in a written contract for security force services.

Comment Summary:
The other commenter recommended that the Commission delete the words “copies of” from 10 CFR 73.55(d)(5)(ii), as the commenter did not believe it is necessary for the NRC to have original versions of reports.

NRC Response:
The Commission disagrees. The NRC has the authority and obligation to retain original copies of any and all documents or records that are required by NRC regulations, whenever the NRC determines that such action is necessary. The Commission has deleted this paragraph but retains this requirement in 10 CFR 73.55(q)(1) “Records”.

Comment Summary:
One commenter stated that the proposed 10 CFR 73.55(e) will require licensees to make significant physical security changes in the OCA.

NRC Response:
The Commission disagrees. The final rule 10 CFR 73.55(b)(4) is revised to clarify the intended scope of this requirement. Each licensee is required to perform a site-specific analysis to determine what measures are needed in the OCA to account for “site” specific conditions relative to the use of physical barriers. The Commission concluded that site-specific conditions directly affect the use, type, function, construction, and placement of physical barriers and therefore, site-specific conditions must be accounted for in the design of the physical protection program.

Comment Summary:

Another commenter noted that proposed 10 CFR 73.55(e) and (e)(3)(iii) require that barriers be "designed and constructed...to deter, delay, and prevent the introduction of unauthorized personnel, vehicles, or materials into areas for which access must be controlled or restricted." The commenter asked: "Since the requirement refers to design, if the NRC approves the plan yet the barrier later fails, can the licensee still conclude that NRC's approval acknowledged that the barrier was, in fact, designed properly?"

NRC Response:
The NRC-approved security plans describe how each licensee will implement NRC requirements at its site. It is the responsibility of each licensee to analyze the site-specific conditions, determine what physical barriers are needed to account for these conditions, and to design and construct physical barriers as needed to perform the intended function to support the physical security program. Construction criteria are site-specific and must be adequate to perform the intended function.

Comment Summary:
Several commenters stated that the Commission should require physical barriers against air attack. One commenter argued that it is unacceptable to exempt air attacks from the kinds of threats reactors must be capable of defending against. The commenter supported either "Beamhenge" shields to prevent planes from crashing into reactor facilities or ground-based air defense systems.

NRC Response:
The Commission has determined that this comment is outside the scope of this section. The final rule 10 CFR 50.54(hh) is added to address threats from aircraft.

Comment Summary:
Another commenter argued that to allow generation of radioactive waste for another twenty years without a permanent storage site picked or the requirement of hardening the waste in a dry cask on site is wrong. The commenter stated that license extensions, if allowed, should be with a condition of hardening the current and future waste.

NRC Response:
The Commission has determined that this comment is outside the scope of this rulemaking.

Comment Summary:
A third commenter stated that recent events have made air attack a continuing issue in the consideration of nuclear plant security. The commenter said that the lack of any provision for security against aerial attack in the proposed rule confirms that the Commission has not asked and is not asking nuclear power plant owners to do anything to resist such attacks. The commenter argued that, apart from this favoritism toward corporate owners, the omission of such defensive measures reflects a profound abdication of responsibility by the NRC itself. The commenter stated that the NRC is aware that in the past seven years al-Qaeda and other terrorist groups have employed plane, missile, and mortar attacks around the world, so not requiring common-sense defensive measures against such attacks reflects either complacency or blindness towards such demonstrated threats.

The commenter stated that the NRC's shortsightedness is also evidenced by its exclusive focus on active defense against attacks involving large commercial aircraft, by its disregard for the

value of preventing damage to a nuclear power plant, and by its dismissal of physical barriers, which provide a passive defense against aerial attack. The commenter said that ignoring general aviation has led the Commission to overlook the potential for using passive physical barriers to protect nuclear power plants from attacks by smaller aircraft and other aerial threats. The commenter said such passive barriers [e.g., appropriately-located grids of vertical and horizontal "I" beams, steel cables, steel mesh curtains, cooling towers, barrage balloons] would reduce or eliminate the "approach avenues" that could be used by larger planes or jets controlled by terrorists.

The commenter also noted that the Commission observed that "active protection against the airborne threat rests with other organizations of the federal government." The commenter said the Commission's observation about other federal agency responsibility for active defense of nuclear power plants against aerial attack is not responsive to a proposal for a physical barrier. The commenter said that, given that the Commission will require physical barriers against water-borne attacks, it similarly should require physical barriers against air attacks.

The commenter noted that there is some risk that an air attack on a nuclear power plant could cause a radiation release that harms people, and a larger risk of a release that could cause enormous economic damage. The commenter concluded that at least some of the risk of air attack can be reduced with physical barriers, and given the potential value of physical barriers against air attack, the Commission should require nuclear power plant owners to install such barriers. The commenter said if this modification requires setting aside or revising the NRC decision on the DBT regulations, then the Commission should do so.

NRC Response:
The Commission added 10 CFR 50.54(hh) to address threats from aircraft.

Comment Summary:
Another commenter said the security requirements must be upgraded to include high-speed attack by a jumbo jet of the maximum size anticipated to be in commercial use, as well as unexpected attack by general aviation aircraft and helicopters. The commenter noted that the requirements must contemplate all such aircraft to be fully loaded, fueled and armed with explosives.

Further, the commenter stated that it is essential that the security requirements take into consideration the cascading consequences of aerial assault on the full spectrum of plant installation and address not only the direct effect of impact, but the full potential after-effects of (A) induced vibrations; (B) dislodged debris falling onto sensitive equipment; (C) a fuel fire; and (D) the combustion of aerosolized fuel (especially in combination with pre-existing on-site gases such as hydrogen).

The commenter concluded that hardening a nuclear power plant against aerial threat will necessitate significant upgrades in plant fortification. However, the commenter noted that even relatively modest measures such as the installation of Beamhenge and the placement of all sufficiently cooled spent fuel into Hardened On-Site Storage Systems would add measurable protection.

NRC Response:

The Commission added 10 CFR 50.54(hh) to address threats from aircraft.

Comment Summary:
One commenter stated that the Commission should require spent fuel pools to revert to low density fuel assembly storage. The commenter stated that licensees should place the remaining assemblies in hardened, dispersed dry cask storage until all assemblies are moved off site.

NRC Response:
The Commission has determined that this comment is outside the scope of this rulemaking.

Comment Summary:
Similarly, another commenter expressed concern that the proposed rule gives no indication that the Commission has taken the most important and effective step necessary to reduce the effectiveness of sabotage against spent-fuel pools, which would be to require licensees to change the configuration of spent-fuel pools from high-density storage to low-density storage using open-frame racks. The commenter argued that the use of low-density storage in spent-fuel pools would dramatically reduce the likelihood that an act of sabotage would cause a fire in a spent-fuel storage pool.

NRC Response:
The Commission has determined that this comment is outside the scope of this rulemaking.

Comment Summary:
Several commenters recommended that the Commission add a physical barrier requirement specific to spent fuel pools.

NRC Response:
The physical barriers discussed in this paragraph are generic to the effectiveness of the physical
protection program. Specific physical barrier requirements are determined through the analysis of site-specific conditions and NRC requirements. In 10 CFR 73.55(e)(7)(v)(B) the Commission specifically requires that the spent fuel pool be protected as a vital area.

Comment Summary:
One commenter stated that spent fuel pools are of particular concern because the disposition of water could uncover the fuel. The commenter stated that if plant workers are unable to effectuate replacement of the water (either because of fire or because they are otherwise incapacitated), experts warn, an exothermic reaction could cause the zirconium clad spent fuel rods to ignite a nuclear waste conflagration that would very likely spew the entire radioactive contents of the spent fuel pool into the atmosphere.

NRC Response:
In 10 CFR 73.55(b)(3) the Commission requires that the physical protection program be designed to prevent significant core damage and spent fuel sabotage. In 10 CFR 73.55(e)(7)(v)(B) the Commission requires that the spent fuel pool be protected as a vital area.

Comment Summary:
A commenter stated that 10 CFR 73.55(e)(1) would require the approved security plans to describe the design, construction and function of physical barriers, including verification that the functional objectives were achieved. The commenter noted that the design, construction, and

function of physical barriers are already described in configuration control documents, such as calculations, drawings, and design basis documents. The commenter argued that it is unnecessary to duplicate information in the PSP that was removed to the references by the PSP format used for DBT. The commenter suggested that Commission delete this requirement and that the information should be retained in the configuration control documents.

Therefore, the commenter recommended that the NRC reword the proposed 10 CFR 73.55(e)(1) to state: "The licensee shall describe in the approved security plans the physical barriers and barrier system functions required to support the licensee's protective strategy".

NRC Response:
The Commission agrees. See also 10 CFR 73.55(e)(2) The Commission has revised the final rule to clarify the scope of this requirement. The Commission concluded that the required description can be satisfied through reference to existing documentation and need not be duplicated in the security plans. This description is subject to the records retention requirements in 10 CFR 73.55(r).

Comment Summary:
One commenter stated that the proposed language is too broad in that it requires all records be retained as safeguards rather than maintaining only those records that meet the definition for being safeguards in accordance with 10 CFR 73.21. The commenter recommended that the NRC replace the phrase "as safeguards" with "that are safeguards".

NRC Response:
The Commission agrees. The Commission has revised final rule text to clarify that this information must be reviewed against the provisions of 10 CFR 73.21 and designated as SGI only where appropriate.

Comment Summary:
Another commenter stated that proposed 10 CFR 73.55(e)(2) would require licensees to protect, as SGI, all physical barrier "analyses, comparisons, and descriptions," which is redundant to the current requirements in 10 CFR 73.21. The commenter noted that, as indicated on page 62695 of the Federal Register notice, this proposed rule was to have replaced the existing 10 CFR 73.55(c)(9)(iii) and (iv). However, the commenter argued that 10 CFR 73.55(c)(9)(iii) and (iv) only address the vehicle barrier system; whereas, proposed 10 CFR 73.55(e)(2), as worded, would apply to all physical barriers constructed to deter, delay, and prevent the introduction of unauthorized personnel, vehicles, or materials into controlled areas.

NRC Response:
The Commission agrees in part. The Commission agrees that the current 10 CFR 73.55(c)(9)(iii) and (iv) are limited to only the vehicle barrier system. However, the Commission has determined that the use of physical barriers at a nuclear power reactor facility is not limited to only vehicle barriers. Physical protection programs also use personnel barriers, delay barriers, channeling barriers, and barriers to provide cover for response personnel. This requirement updates the regulatory framework for physical barriers to generically reflect how they are used within the physical protection program. Therefore, the Commission concluded

that this requirement has been and continues to be a standard practice that is currently applied by licensees and therefore, has no impact.

Comment Summary:
The commenter also argued that without the current 10 CFR 73.55(c)(8) wording, one would never understand what is meant by the term “comparisons” and that “comparisons” can be considered part of the barrier “analyses.”

NRC Response:
The Commission agrees. The Commission has revised the final rule to delete the reference to comparisons because this pre-existing term is no longer needed. The final rule requires that each barrier be designed and constructed to account for site-specific conditions and perform the intended function rather than a specific baseline against which a comparison can be made.

Comment Summary:
In addition, the commenter argued that licensees can no longer protect the physical barrier descriptions since most are in plain view by the public and all are in view of site workers. Also, the design, fabrication and placement drawings for barriers do not generally need to be SGI because the barriers themselves are generally in the open, subject to observation. The commenter argued that what must be protected are the “analyses” and functional requirements which describe the design criteria which, if disclosed to the public, could assist an adversary in an act of radiological sabotage.

NRC Response:
The Commission disagrees with the suggestion that because a physical barrier is “in plain view by the public” or otherwise exposed to observation, then all associated design and fabrication criteria can also be obtained through observation. The Commission has revised final rule text to clarify that this information must be reviewed against the provisions of 10 CFR 73.21 and designated as SGI only where appropriate.

Comment Summary:
The commenter suggested that the NRC reword proposed 10 CFR 73.55(e)(2) to state: “The licensee shall retain in accordance with 10 CFR 73.70, all analyses and functional requirements of the physical barriers and barrier systems used to satisfy the requirements of this section.” Or, the commenter suggested that NRC reword proposed 10 CFR 73.55(e)(2) to state: “The licensee shall retain in accordance with 10 CFR 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 as safeguards information in accordance with the requirements of 10 CFR 73.21, if the unauthorized disclosure of such analyses and descriptions could reasonable be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of source, byproduct, or special nuclear material.”

NRC Response:
The Commission agrees in part. The Commission has revised the final rule to be consistent with the suggested changes, however, the Commission disagrees with the suggested rule text beyond a clear reference to the criteria in 10 CFR 73.21.

Comment Summary:

In 73.55(e)(3)(i), one commenter stated that the term “clearly delineate” is not defined and can be interpreted broadly. The commenter stated that this requirement is ambiguous (e.g., does it mean signage at the ditch, signage on the water, signage on the barrier, markings on a site layout drawing, etc.). Also, the commenter stated that there are no performance criteria in this section and suggested that the Commission delete this provision from the final rule. However, if retained, the commenter suggested that the Commission clarify the meaning and intent of “clearly delineate the boundaries of the area” in the SOCs.

NRC Response:
The Commission agrees. The phrase “clearly delineate” was intended to simply and generically describe a requirement to ensure that the barrier is placed or prominently displayed, at a location where its presence would clearly identify where the area to be controlled begins. The Commission intended this requirement to provide the flexibility needed for each licensee to account for site-specific conditions and to answer the questions presented by the commenter (i.e., does it mean signage, markings, etc?). Upon review, the Commission has determined that this requirement is better addressed in guidance and therefore, the Commission has deleted this requirement from the final rule.

Comment Summary:
Another commenter stated that proposed 10 CFR 73.55(e)(3)(i) adds a requirement to delineate the boundaries of the areas for which the physical barrier provides protection. The commenter argued that, as worded, the proposed requirement appears to require marking the physical barrier or plant area, which is contrary to the need-to-know for SGI. If the intent is to include in the boundary delineation in either the PSP or barrier analyses, then this would duplicate the configuration control documentation. Therefore, the commenter suggested that the Commission delete this provision from the final rule.

NRC Response:
The Commission agrees in part. Upon review, the Commission has determined that this requirement is better addressed in guidance and therefore, the Commission has deleted this requirement from the final rule.

Comment Summary:
One commenter stated that 10 CFR 73.55(e)(3)(ii) is well-written and performance-based, but the SOC language is confusing and the Commission should revise it as follows: “This requirement would be added to apply the current requirement of 10 CFR 73.55(c)(8) to all barriers. The Commission's view is that the physical construction, materials, and design of any barrier must be sufficient to perform the intended function and therefore, the licensee must meet these standards.”

NRC Response:
The SOCs attempted to clarify that the pre-existing requirement 10 CFR 73.55(c)(8) is specific to vehicle barriers only, however, the Commission's expectation is that all barriers, not just vehicle barriers, will meet the final rule design goal/performance-criteria of performing the intended function, rather than a specific baseline construction standard. The Commission concluded that such flexibility is necessary to allow each licensee to account for site-specific conditions.

Comment Summary:

A commenter stated that the physical barriers must function consistently with the site protective strategy, which does not always require them to perform all three functions (i.e., visual deterrence, delay, and support access control measures). The commenter recommended that the NRC revise 10 CFR 73.55(e)(3)(iii) to replace “and support” with “or support”.

NRC Response:
The Commission agrees that physical barriers must function consistently with the site protective strategy and that all three performance-criteria may not be required of every barrier in every case. Nonetheless, any one criterion will apply to any one intended function, and therefore, each one is valid by itself. The Commission has revised the final rule to clarify the performance-criteria for this requirement.

Comment Summary:
Another commenter stated that the provision adds a new requirement for physical barriers to provide visual deterrence. The commenter argued that this requirement is unnecessary to demonstrate an effective protective strategy, was not part of the DBT, and has not been a specific design objective. The commenter noted that in many cases, the design details that make a barrier formidable have been deliberately hidden to enhance its effectiveness. The commenter concluded that without specific guidance, it is unclear what existing physical barriers meet this requirement. Therefore, the commenter suggested that the Commission delete this provision from the final rule.

NRC Response:
The Commission agrees in part. The Commission disagrees that this is a new requirement and disagrees with the recommendation to delete this requirement. The use of physical barriers for “visual deterrence” is a long-standing professionally accepted application. Nonetheless, the Commission agrees that the term "visual" is not necessary and has deleted the term "visual" from the final rule.

Comment Summary:
A commenter stated that 10 CFR 73.55(e)(10) is inconsistent with the existing regulations and associated regulatory guidance for openings in the PA and VA. First, the commenter said the word “unattended” is confusing and the commenter recommended that the Commission delete it from the final rule. Second, the commenter stated that this requirement would inappropriately apply the 620 cm^2 (96.1 in^2) or greater requirement to the vehicle barriers, which is impracticable. Third, the commenter stated that none of the security Orders included such a requirement. The commenter recommended that the Commission should revise the provision to state: “Unattended openings in the protected area or vital area barrier established to meet the requirements of this section that are 620 cm^2 (96.1 in^2) or greater in total area and have a smallest dimension of 15 cm (5.9 in) or greater, must be secured or monitored at a frequency that would prevent exploitation of the opening consistent with the intended function of each barrier.”

NRC Response:
The Commission agrees in part. The Commission has determined that “Unattended Openings” are appropriately addressed in RIS 2002-05 and, therefore, need not be addressed by this requirement. The Commission has revised this requirement to generically address openings in any barrier and the need to secure and monitor these openings is dependent upon the intended function to be performed by the barrier and the ability to exploit the opening. This requirement

is intended to establish performance-criteria for barriers to ensure that barrier openings can not be exploited to defeat the intended function of that barrier. The Commission has revised the final rule to delete the specific opening size of 620 cm^2 (96.1 in^2) or greater because this dimension is specific to personnel barriers and would be inclusive to this requirement only for barriers that are intended to prevent access by persons.

Comment Summary:
Another commenter stated that 10 CFR 73.55(e)(10) would be applied to all barriers, even those in the OCA, to include the vehicle barrier system. The commenter stated that that none of these barriers were designed to meet the 96 in^2 opening requirements, which have historically only been applied to PA and VA openings. In addition, the commenter noted that the opening dimensions must reflect those specified in NUREG-0908, "Acceptance Criteria for the Evaluation of Nuclear Power Reactor Security Plan," since this was the NRC guidance utilized to design licensee's PA and VA barriers.

The commenter stated that there are two problems with this proposed requirement. First, the limitations make no sense if applied to the vehicle barriers covered by the proposed 10 CFR 73.55(e), since the objective of such barriers is to exclude vehicles, not people. Second, the dimensions cited differ from the current requirements of 96 in^2 with 6 inch or greater opening, such that the existing PA and VA barriers would have to be re-evaluated and modified if needed.

Therefore, the commenter recommended that the Commission clarify the provision as applying only to PA and VA barriers. The commenter suggested that the Commission revise the provision to state: "Unattended openings in either a protected or vital area barrier established to meet the requirements of this section that are 96 in2 or greater in total area and have the smallest dimension as 6 in or greater, must be secured or monitored at a frequency that would prevent exploitation of the opening consistent with the intended function of each barrier".

NRC Response:
The Commission agrees. The Commission has revised this requirement to generically address openings in any barrier and the need to secure and monitor these openings is dependent upon the intended function to be performed by the barrier and the ability to exploit the opening. This requirement is intended to establish performance-criteria for barriers to ensure that barrier openings can not be exploited to defeat the intended function of that barrier. The Commission has revised the final rule to delete the specific opening size of 620 cm^2 (96.1 in^2) or greater because this dimension is specific to personnel barriers and would be inclusive to this requirement only for barriers that are intended to prevent access by persons.

Comment Summary:
One commenter stated that 10 CFR 73.55(e)(10) imposes requirements on "any barrier established to meet the requirements of this section" when the requirement is clearly not applicable to all such barriers.

NRC Response:
The NRC agrees. The Commission has revised the final rule to delete the specific opening size of 620 cm^2 (96.1 in^2) or greater because this dimension is specific to personnel barriers and would be inclusive to this requirement only for barriers that are intended to prevent access by persons..

Comment Summary:
One commenter stated that the proposed 10 CFR 73.55(e)(6)(v), as worded, would require some facilities to submit exemptions to meet the rule requirements. The commenter noted that the SOC adds a requirement that all construction features of the control room, central alarm station, and last point of control for PA access must be bullet resisting. The commenter stated that the proposed requirement is not performance-based and rather than support the proposed rule that simply requires these spaces to be bullet resisting, it appears to exclude existing bullet resisting configurations composed of overlapping but discontinuous bullet resistant walls or multiple walls in series to meet the bullet resisting requirement. Therefore, the commenter suggested that the Commission revise the SOC to support the performance-based objective of the proposed rule, without reference to "all construction features." Also, the commenter suggested that the Commission add the phrase "as described in the approved physical security plan" to the end of the provision.

NRC Response:
The Commission disagrees. This requirement is a retained pre-existing requirement. The SOC generically addresses all construction because a listing of all possible features is not practical.

Comment Summary:
Another commenter stated that the Commission should define the level of the bullet-resisting barrier. The commenter noted that a common definition used is the National Institute of Justice (NIJ) standards and a good recommendation for the control room envelope would be at least NIJ level IV bullet resistance.

NRC Response:
The Commission disagrees. The NRC bullet resisting standards and criteria have been provided to licensees in guidance. The Commission has determined that specific bullet-resisting standards are appropriately addressed in guidance, and therefore, the Commission disagrees that a specific bullet-resisting standard should be specified in this rule text.

Comment Summary:
Three commenters referred to the proposed 10 CFR 73.55(e)(4). One commenter stated that this new provision is more stringent than any requirements contained in the Orders and is a significant impact on industry which was not evaluated in the Regulatory Analysis. The commenter noted that the only barriers in the OCA are vehicle barriers to provide standoff for vehicle bombs. Further, the commenter stated that the language in proposed 10 CFR 73.55(e)(8) addresses vehicle barriers and thus adequately captures existing requirements for physical barriers in the OCA.

Also, the commenter argued that the following terms are not defined in 10 CFR 73.2 and are ambiguous: "unauthorized access," "unauthorized activities," and "approach routes to the facility." If the Commission retains this provision, the commenter recommended the Commission revise it as follows: "The licensee shall establish and maintain physical barriers in the OCA to support effective implementation of the licensee's protective strategy".

NRC Response:
The Commission agrees in part. The Commission disagrees that this requirement is new and disagrees that it is more stringent than pre-existing requirements. However, the Commission

has revised the final rule to delete the terms addressed by this comment and to clarify that the focus is on the design of the physical protection program and protective strategy.

The Commission disagrees that all sites have only vehicle barriers in the OCA. The types of barriers needed in the OCA can include vehicle barriers, channeling barriers, delay barriers, or even personnel barriers if site-specific conditions necessitate such measures to protect the facility against the DBT, prevent significant core damage and spent fuel sabotage, or otherwise maintain the capability to protect against radiological sabotage. Therefore, the need for physical barriers in the OCA is determined by each licensee through the analysis of site-specific conditions.

Comment Summary:
Another commenter stated that the standards to "deter, delay, prevent..." for the OCA are as rigorous as the standards for the PA barrier and will, in a sense, require that the entire barrier/border concept built into the PA be moved out to the OCA. The commenter argued that this would be a tremendous additional expense for the licensees.

NRC Response:
The Commission agrees in part. The Commission agrees that the same performance-criteria, applies to each type of physical barrier as needed to perform its intended function, however, the need for that function/barrier in the OCA is site-specific. Therefore, the Commission disagrees that this would the PA to be moved out to the OCA.

Comment Summary:
A third commenter stated that the proposed 10 CFR 73.55(e)(4), as worded, implies that licensees must have physical barriers in the OCA, which could be interpreted as requiring personnel barriers to prevent unauthorized access by personnel. The commenter stated that this is a new requirement. The commenter argued that the expectation to deter, delay, or prevent unauthorized access and facilitate early detection in the OCA is unnecessary to demonstrate an effective defensive strategy and cannot be implemented due to the congested layout and/or geography at many sites. Therefore, the commenter suggested that the Commission either delete this provision or reword it to be consistent with existing requirements to state: "The licensee shall establish and maintain vehicle barriers in the owner controlled area to deter, delay, or prevent unauthorized vehicle access, facilitate the early detection of unauthorized vehicular activities, and control vehicle approach routes to the facility".

NRC Response:
The Commission disagrees that this is a new requirement and that this requirement can not be implemented. The Commission agrees that each site is different and that while one site may have a congested OCA, another site may not. This is why each site is required to analyze their site-specific conditions and determine what measures are needed to support an effective physical protection program in the OCA. As such, a determination of what measures are needed in the OCA directly affects the licensee capability to protect against the DBT.

Comment Summary:
One commenter stated that, in 10 CFR 73.55(e)(5)(i)(A), the use of the term "unobstructed" is not performance-based and the Commission should reword the provision to state: "Designed and of sufficient size to permit assessment of activities on either side of the PA barrier."

NRC Response:
The Commission agrees in part. The NRC intended the term “unobstructed’ to clarify the pre-existing 10 CFR 73.55(c)(3) requirement to “observe activities” on either side of the isolation zone (IZ). The NRC's expectation is that an IZ will be designed to ensure activities can be observed on either side of the PA perimeter. To accomplish this each licensee must account for obstacles that would prevent this observation and design the IZ to ensure timely and accurate observation or assessment of activities can be made. The Commission has revised the final rule to delete the term “unobstructed” from this requirement because the requirement to provide observation on either side of the PA perimeter sufficiently establishes the desired performance that was intended by the term "unobstructed."

Comment Summary:
Similarly, one commenter stated that the word “unobstructed” adds nothing to the performance objectives of proposed 10 CFR 73.55(b) and requirements of 10 CFR 73.55(e)(3), but is overly prescriptive and contrary to the stated consideration of “provid[ing] a more performance-based requirement.”

NRC Response:
As stated above, the NRC agrees in part.

Comment Summary:
A commenter also stated that 10 CFR 73.55(e)(5)(i)(A) requires as isolation zone on both sides of the PA barrier regardless of a licensee’s current approved PA barrier configuration. The commenter argued that this requirement is unnecessary to achieve an effective protective strategy. In addition, the commenter noted that this contradicts the proposed 10 CFR 73.55(e)(6)(iv) that exempts isolation zones in certain cases. Therefore, the commenter suggested that the Commission modify the proposed 10 CFR 73.55(e)(5)(i)(A) to take into consideration the exemption for having obstructions in the isolation zone. The commenter suggested the following language: “Designed and of sufficient size to permit unobstructed observation and assessment of activities on either side of the protected area barrier except as noted in 10 CFR 73.55(e)(6)(i).”

NRC Response:
The Commission disagrees. The current requirement in 10 CFR 73.55(c)(3) is retained with only minor revisions. The isolation zone is required to be maintained in outdoor areas adjacent to the PA perimeter. Obstructions that prevent observation would mean that this requirement is not met. The NRC disagrees that the relief stated in the proposed 10 CFR 73.55(e)(6)(i) negates the need for observation. The requirement to observe activities on both sides of the PA perimeter remains applicable at all times. Where a building is part of the PA perimeter an isolation zone is not needed provided appropriate barriers are installed and observation requirements are met.

Comment Summary:
With respect to 10 CFR 73.55(e)(5)(i)(B), one commenter stated that assessment equipment and capabilities are more appropriately addressed in proposed 10 CFR 73.55(e)(5)(ii) and should be deleted from this paragraph. Additionally, the commenter stated that evaluation of the detected activity before completed penetration of the PA barrier is more appropriately addressed in proposed 10 CFR 73.55(e)(5)(ii) (i.e., “before and after each alarm annunciation.”). The commenter suggested that the Commission delete the following phrase from the provision:

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

NRC Response:
The Commission agrees in part. The Commission agrees that detection and assessment equipment should be addressed individually. Therefore, the Commission has revised the final rule to separate detection equipment versus assessment equipment. Assessment is addressed in the final rule 10 CFR 73.55(e)(5)(i)(C). The Commission disagrees that the requirement for detection "before completed penetration of the protected area perimeter barrier" should be deleted and has retained this requirement in the final rule 10 CFR 73.55(e)(7)(i)(B). The Commission's expectation is that detection will occur before the PA perimeter is penetrated and that the use of video-capture will allow the licensee to assess the cause of the alarm for the period of time preceding the penetration.

Comment Summary:
Another commenter stated that the proposed 10 CFR 73.55(e)(5)(i)(B) contains a new requirement that assessment equipment facilitate evaluation of unauthorized activities before PA barrier penetration. The commenter stated that this requirement is misplaced in this section, is infeasible, and is contrary to the stated consideration of "provid[ing] a performance-based requirement." The commenter argued that specific design requirements for intrusion detection system (IDS) equipment and assessment equipment should be contained in the proposed 10 CFR 73.55(i) rather than this section. The commenter noted that some scenarios presently envisioned under the DBT, as well as others under consideration, cannot be evaluated before PA barrier penetration and modifications to the DBT may be promulgated outside of 10 CFR part 73. The commenter concluded that the Commission should modify the proposed 10 CFR 73.55(e)(5)(i)(B) to be more consistent with current 10 CFR 73.55(c)(4).

NRC Response:
The Commission disagrees that this is a new requirement. However, the Commission has revised the final rule to separate detection equipment versus assessment equipment.

Comment Summary:
Another commenter stated that the proposed 10 CFR 73.55(e)(5)(i)(B) requires IDS equipment capable of evaluation of unauthorized activities "before completed penetration." The commenter noted that the NRC's own tests and research acknowledge that penetrations of the PA barrier can be accomplished by skilled adversaries in less than 2 seconds, and also acknowledge that a skilled CAS operator would take longer than 2 seconds to locate the appropriate monitor that is alarming, much less perform the evaluation. Therefore, according to the NRC's own research, the commenter concluded that it is impossible to meet this standard.

NRC Response:
As stated above, the Commission agrees in part. Therefore, the Commission has revised the final rule to separate detection equipment versus assessment equipment.

Comment Summary:
One commenter stated that the proposed 10 CFR 73.55(e)(5)(ii) appears to refer to video capture, but does not specifically mention it.

NRC Response:
The Commission agrees. This requirement is written with performance-based language that is

intended to generically describe the technology that is currently known as video-capture.

Comment Summary:
Similarly, another commenter stated that the proposed 10 CFR 73.55(e)(5)(ii) and associated SOCs add a new requirement for video capture. The commenter stated that this requirement is not performance-based, and the performance-based requirement would be for assessment features “as needed” to implement an effective protective strategy.

Also, the commenter noted that it is unclear whether the requirement would apply only to primary assessment capability, or both primary and backup capabilities. The commenter argued that video capture is not needed on the primary system or the backup system if the protective strategy is effective without it. Therefore, the commenter recommended that the Commission revise this section to achieve a performance-based requirement for assessment features “as needed” to implement an effective protective strategy. The commenter suggested adding the phrase “as needed to implement an effective protective strategy” to the end of the provision.

NRC Response:
The Commission disagrees. The Commission agrees that this is a new requirement for video capture as is stated in the proposed rule federal register notice (FR 62670). The Commission does not, however, distinguish between primary and back-up systems herein, because back-up systems are understood to be compensatory measures taken in response to a system failure. The Commission agrees that a licensee may choose an alternative measure for satisfying this requirement, however, this requirement captures pre-existing licensee practices regarding use of this equipment and is appropriate to update the NRC's regulations regarding this technology and its use at both pre-existing and future nuclear power reactor facilities. This requirement addresses IZ assessment equipment of which the Commission has determined is a pre-existing licensee application.

Comment Summary:
One commenter stated that the proposed 10 CFR 73.55(e)(5)(iii) and associated SOCs add a requirement to maintain the areas inside, outside, and adjacent to the PA barrier clear of obstructions. The commenter stated that this requirement is not performance-based, and precludes use of the areas inside the PA barrier for laydown (the performance-based requirement would be for maintaining assessment capability).

The commenter stated that the proposed SOC section would have a significant negative impact on plant operation for sites with small PA footprints. Therefore, the commenter stated that the Commission should reword this provision to achieve a performance-based requirement to control laydown activities within the PA to maintain assessment capability at the PA barrier.

NRC Response:
The Commission agrees in part. This requirement is necessary to ensure that the observation and assessment requirements of this section are effectively satisfied. The pre-existing requirement to locate parking facilities outside of the IZ has been updated to ensure that licensee’s account for the observation requirements for the IZ when determining the locations to be used for laydown rather than precluding this practice, as is suggested by this commenter. The Commission has revised the final rule to clarify that the focus of this requirement is to not have obstructions inside the IZ. The Commission's expectation is that each licensee will

account for any obstructions by configuring assessment tools to ensure the ability to "see around" the obstruction and thereby, satisfying the performance-criteria of this requirement.

Comment Summary:
One commenter noted that proposed 10 CFR 73.55(e)(6)(i) is a new requirement and the current PA barrier requirements satisfy the protection of these penetrations. To more closely align with current design requirements, the commenter recommended that the Commission revise the provision as follows: "The protected area perimeter must be protected by physical barriers designed and constructed to meet Commission requirements and penetrations through this barrier, greater than those allowed by (e)(10), must be secured in a manner that prevents, delays, or detects the exploitation of any penetration." The commenter added that meeting this requirement for smaller penetrations is not necessary.

NRC Response:
The Commission agrees in part. The Commission disagrees that this is a new requirement and has determined that this requirement is an appropriate update to the regulatory framework. However, the Commission agrees that this requirement could include penetrations smaller than those addressed in 10 CFR 73.55(e)(10), but only where that size opening could be exploited to defeat the intended function of the barrier. The performance-criteria for all barriers is directly contingent upon the intended function of that barrier and, therefore, any size opening that can be exploited to defeat the purpose of the barrier is unacceptable and must be secured and monitored.

Comment Summary:
Another commenter stated that use of the language "penetrations ... must be secured in a manner that prevents or delays, and detects ..." is ambiguous, duplicative and potentially contradictory to the more clearly stated proposed language of 10 CFR 73.55(e)(10). The commenter noted that one can infer from the SOCs that the intended meaning of 10 CFR 73.55(e)(6)(i) is that an exploitation scenario that is prevented must nevertheless be detectable, which would indicate a wasteful approach antithetical to program effectiveness. Therefore, the commenter suggested that the Commission reword the provision to state: "The protected area perimeter must be protected by physical barriers designed and constructed to meet Commission requirements as specified in the Commission-approved security plan."

NRC Response:
The Commission disagrees that the requirement to detect an attempt to exploit a PA penetration would indicate a wasteful approach antithetical to program effectiveness. The pre-existing requirement in 10 CFR 73.55(c)(4) states, "Detection of penetration or attempted penetration of the protected area or isolation zone...". The Commission has determined that, as written, this provision retains and is consistent with this pre-existing requirement. In addition, the Commission disagrees with the recommended rule text change because Commission requirements are stated in the regulations, not in approved security plans.

Comment Summary:
Another commenter noted that PA barriers are required to be "designed and constructed to meet Commission requirements." The commenter asked: What are these specific requirements? Is this something that is going to be detailed in guidance? If so, given the wide range of possible outcomes, how can the industry and public comment on this section without knowing what those specific requirements are?

NRC Response:
Commission requirements for the design and construction of physical barriers are performance-based such that the licensee is responsible to construct, install, and maintain physical barriers that are designed to perform a stated function within the physical protection program. The specific design and construction of a barrier is determined by site-specific conditions and is predicated upon the intended function to be performed.

Comment Summary:
One commenter stated that the proposed 10 CFR 73.55(e)(6)(iii) does not match most facility PA configurations and is more appropriate for VA portals which contain “crash bars;” whereby, upon emergencies, personnel can bypass the portal locking devices for emergency exit only, but the portal will alarm upon exiting this way. Therefore, the commenter suggested that, since PA turnstiles do not alarm upon emergency exiting, the Commission should revise the proposed 10 CFR 73.55(e)(6)(iii) to replace the term “protected area” with “vital area” and replace “alarmed” with “alarm upon an emergency exit.” Or, the commenter suggested that the NRC could reword the provision to allow dual-use entry/exit portals that can be unlocked for emergency exit while still prohibiting unauthorized entry.

NRC Response:
The Commission agrees. The Commission has revised the final rule and the SOCs to clarify the scope of this requirement and to eliminate unintended implications. Although not desired, the Commission agrees that dual use portals may be designated as emergency exits, however, it is important to note that where such dual use portals are used for entry and emergency exit, all NRC requirements for access/entry apply. In addition, when not attended, emergency exits must be locked and alarmed to delay and detect unauthorized entry into the PA or VA. The Commission agrees that PA turnstiles need not be alarmed because they are not unattended. However, the Commission disagrees that this requirement only applies to VAs and is consistent with the pre-existing 10 CFR 73.55(e)(3) which applies to both PA and VA.

Comment Summary:
For 10 CFR 73.55(e)(6)(iv), a commenter stated that the list of barrier components includes walls and roofs, but the inclusion of penetrations seems incorrect here. The commenter noted that a penetration is typically thought of as an engineering, operational, or construction necessity (e.g., a drainage pipe). If penetration, in this requirement, is meant to refer to personnel and vehicle portals, the commenter suggests that the provision clearly specify this. Otherwise, the commenter argued that the traditional protections for penetrations (i.e., drainage pipes, etc.), such as locks and alarms, would not be consistent with the current requirement.

NRC Response:
The Commission agrees. The Commission has revised the final rule to delete "or penetrations" from the final rule.

Comment Summary:
One commenter stated that 10 CFR 73.55(e)(6)(vi) is not consistent with the Orders and the security plan template. The commenter recommended that the Commission replace the word “All” with “Appropriate.”

NRC Response:
The Commission disagrees. The word “all” is retained from the pre-existing 73.55(c)(4). The

proposed rule mistakenly did not identify the pre-existing rule text as the basis of this requirement. The pre-existing 10 CFR 73.55(c)(4) states “All exterior areas within the protected area shall be periodically checked to detect the presence of unauthorized persons, vehicles, or materials. As the term “All” is a pre-existing requirement, it is retained without revision. However, the Commission has added a provision for relief where site-specific conditions preclude meeting this requirement for safety reasons.

Comment Summary:
Another commenter stated that 10 CFR 73.55(e)(6)(vi) adds a requirement to periodically check all exterior areas within the PA for unauthorized activities, personnel, vehicles and materials. The commenter argued that this provision would be impossible to comply with in all cases since some PA exterior areas are not accessible due to either safety or limited access considerations. The commenter noted that the proposed requirement is not performance-based, and is unclear as to the level or periodicity of the search that would be expected.

In addition, the commenter notes that with all the existing security controls in place (e.g., designated/non-designated vehicle controls, PA intrusion detection/assessment capabilities, PA closed-circuit television (CCTV), PA badging/access controls, fitness-for-duty (FFD) program, BOP, Access Authorization and Control Program, Insider Mitigation Program, material/personnel/vehicle search requirements), a new requirement such as this one is overkill and serves no valid protective purpose. Therefore, the commenter suggested that the Commission delete this provision from the final rule.

NRC Response:
As stated above, the Commission disagrees that this is a new requirement. The word “all” is retained from the pre-existing 10 CFR 73.55(c)(4).

Comment Summary:
Another commenter asked: Can the exterior areas within the PA that must be periodically checked for unauthorized activities be checked by CCTV? How about IDS? If not, the commenter said the Commission should change the wording of 10 CFR 73.55(e)(6)(vi) .

NRC Response:
Consistent with the proposed 10 CFR 73.55(i)(5) and (i)(6), the use of electronic video equipment to accomplish the periodic checks is an acceptable supplement to patrols but is not sufficient, in-and-by itself.

Comment Summary:
Two commenters stated the cross-reference in 10 CFR 73.55(e)(7)(i) to proposed 10 CFR 73.55(f)(2) is an error. One of the commenters stated that this provision requires that VA barriers be designed and constructed to perform their required function, except according to paragraph (f)(2). However, (f)(2) refers to cyber attacks, which have little or nothing to do with VA barriers (except at the personnel portals).

NRC Response:
The Commission has deleted this reference in the final rule as it is not necessary. The correct reference is the proposed 10 CFR 73.55(f)(3).

Comment Summary:

The other commenter stated that the correct reference is 10 CFR 73.55(t).

NRC Response:
The Commission has deleted this reference in the final rule as it is not necessary. The correct reference is the proposed 10 CFR 73.55(f)(3).

Comment Summary:
Another commenter supported proposed 10 CFR 73.55(e)(7)(i), which requires vital equipment be located only in VAs. The commenter noted that at Three Mile Island (TMI) the control room air intake building has been located in the PA -- the licensee was able to rationalize this over a conflict of what constitutes "vital equipment." The commenter concluded that control room operators must be protected from incapacitating agents.

NRC Response:
The Commission has determined that this comment is outside the scope of this rulemaking.

Comment Summary:
One commenter stated that 10 CFR 73.55(e)(7)(v) inappropriately includes the phrase "all vital areas," which is confusing and above and beyond the requirements in the current regulations and Orders. The commenter noted that the correct reference in the current regulations is 10 CFR 73.55(d)(7)(i)(D), which addresses access to all VAs. The commenter stated that this requirement should more appropriately focus on all VA access portals and emergency exits.

Additionally, the commenter stated that the requirement that "emergency exit locking devices shall be designed to permit exit only" may be construed to mean that keys cannot be used from outside. If this is the case, it could impact operations and security emergency response and security defensive strategies that rely on responders entering the VA through the emergency exit with the use of a security controlled key. Therefore, the commenter suggested that the Commission revise the provision to state: "The licensee shall protect all vital area access portals and vital area emergency exits with intrusion detection equipment and security controlled locking devices."

NRC Response:
The Commission agrees. The correct pre-existing requirement upon which this requirement is based, is 10 CFR 73.55(d)(7)(i)(D). The Commission's intent regarding emergency exits was based on a literal application of the term "as a penetration that is used for egress only." The Commission acknowledges that this proposed requirement did not account for current licensee vital area entry/exit procedures that require individuals to "card-out" as well as card-in. Therefore, the Commission has revised the final rule to allow the use of entry/exit portals as emergency exits as is pre-existing licensee practice. The term "vital areas" has been deleted to clarify that the intended focus of this requirement is on portals and not the interior areas of a vital area.

Comment Summary:
Another commenter stated that proposed 10 CFR 73.55(e)(7)(v) is not performance-based (a performance-based requirement would be to demonstrate an effective protective strategy). The commenter argued that VA IDS adds no significant capability for the DBT if the VA portals are alarmed and the remaining barriers are substantial enough to require explosive breach (turbine grating, concrete walls, etc.).

In addition, the commenter noted that it is not feasible to backfit VA barrier IDS into existing facilities, particularly where the barrier is a wall with equipment on both sides (e.g., the walls between the turbine building and adjoining vital structures). Therefore, the commenter recommended that the NRC delete the added requirement for VA IDS. Also, the proposed requirement for emergency exit locking devices should be revised for consistency with the existing use of solenoid-controlled VA portals, which can be opened in one direction to allow emergency exit, while still remaining locked from the outside prohibiting unauthorized entry.

NRC Response:
The Commission agrees in part. The term “vital areas” has been deleted to clarify that the intended focus of this requirement is on portals and not the interior areas of a vital area. Additionally, the Commission has revised the final rule to allow the use of entry/exit portals as emergency exits as is pre-existing licensee practice.

Comment Summary:
One commenter stated that the proposed provision expands the requirements beyond those required by the current rule and Orders. The commenter noted that, specifically, it expands the requirement pertaining to “secondary power supply systems” from just “alarm annunciator equipment” to all “intrusion detection and assessment equipment”. The commenter argued that the need for such a significant expansion is not explained nor is it supported by the NRC Force-on-Force inspections completed to date. Therefore, the commenter suggested that Commission revise the provision by replacing “intrusion detection and assessment” with “alarm annunciator.”

NRC Response:
The Commission agrees in part. Upon review, the Commission concluded that the proposed requirement would have unintentionally expanded the requirement to protect all IDS and assessment equipment back-up power sources as VAs. Upon review the Commission concluded that not all IDS and assessment equipment are connected to the same secondary power source required by the pre-existing 10 CFR 73.55(e)(1) for alarm annunciation equipment. Therefore, the proposed rule would have would have required that the back-up power sources for each component or grouping of IDS and assessment equipment be protected as a VA. This consequence goes beyond the Commission’s intent.

The Commission intended only to update the regulatory framework to require back-up power for IDS and assessment equipment consistent with the use of this technology. Alarm annunciation equipment is one component within the intrusion detection and assessment "system" and all other components of that system must also operate from back-up power to generate the signal needed to activate annunciation equipment.

To clarify the NRC's intent and expectations, the Commission has revised the final rule in 10 CFR 73.55(e)(9)(vi)(A) to retain the pre-existing 10 CFR 73.55(e)(1) requirement that secondary power supply systems for alarm annunciation equipment must be protected as “vital equipment,” located in a vital area. Additionally, the Commission has added 10 CFR 73.55(i)(3)(vii) to independently address back-up power for IDS and assessment equipment and to clarify that these back-up power supplies need not be protected as vital equipment.

The Commission has determined that addressing only secondary power for “alarm annunciator

equipment” is no longer technically correct and does not accurately represent the use of this technology. The Commission has concluded that, to ensure that an alarm is generated and that an assessment of each alarm can be made, all components within the intrusion detection and assessment system, such as sensors, routers, multiplexers, cameras, etc., must also function through back-up power. Without back-up power to all supporting equipment within the “system”, the signal required to activate the alarm annunciation equipment and make an assessment of the cause of the alarm, would not be generated, and therefore, detection will not occur, rendering the secondary power supply to "annunciation equipment" useless.

Comment Summary:
Another commenter stated that it is unclear how proposed 10 CFR 73.55(e)(7)(iii) would apply to the outside of the spent fuel pool walls. It is the walls, rather than the equipment within, that are of interest for spent fuel sabotage, which requires uncovering the fuel. The commenter noted that the outside of the spent fuel pool walls are in non-VAs at many facilities. However, the walls may be bunkered to prevent breach by DBT threats below the top of the spent fuel, and/or grade level at the non-vital walls may be above the elevation at which spent fuel sabotage could occur. Therefore, the commenter suggested that the Commission revise this provision to clarify that it applies only to the inside of the spent fuel pool. The commenter stated that if the Commission’s intent is to include the outside of the walls as well, then clarification is needed that this only applies to portions of the walls where breach by the DBT threat could credibly result in spent fuel sabotage.

NRC Response:
The Commission disagrees. This requirement does not intend to address the unique construction concerns that are associated with spent fuel pools but rather simply requires that the interior of a spent fuel pool structure, be protected as a vital area. The exterior of the spent fuel pool is inside the protected area and is afforded protection against unauthorized activities.

Comment Summary:
One commenter stated that 10 CFR 73.55(e)(7)(iv) is redundant to proposed 10 CFR 73.58 and should be deleted to eliminate any confusion that this requirement goes beyond the requirements in 10 CFR 73.58. The commenter stated that limited compensatory actions, if needed, per proposed 10 CFR 73.58 would more appropriately address maintenance on vital equipment. Therefore, the commenter recommended that the Commission delete this provision from the final rule.

NRC Response:
The Commission agrees. The Commission has deleted this requirement from the final rule to avoid unintended duplication and impact beyond current requirements. The Commission's expectation is that licensees will ensure that the potential impact of out-of-service conditions is analyzed and appropriate actions are taken if needed.

Comment Summary:
One commenter stated that the header should clarify that 10 CFR 73.55(e)(8) applies only to land-based vehicles.

NRC Response:
In the final rule, the Commission has revised this section (now 10 CFR 73.55(e)(10)) to generically address vehicle control measures as part of the physical protection program design. The final rule in 10 CFR 73.55(e)(10)(i) addresses land vehicles, and the final rule in 10 CFR

73.55(e)(10)(ii) addresses waterborne vehicles.

Comment Summary:
One commenter stated that licensees must protect against vehicle bombs with a force of up to 20,000 lbs. of explosives and account for the ground shock wave which can overcome earthquake proofing measures.

NRC Response:
The NRC has determined that this comment is outside the scope of this rulemaking and is addressed by the Commission in 10 CFR 73.1 "Design Basis Threat".

Comment Summary:
Another commenter stated that a land vehicle should not be limited to a four-wheeled drive car or truck, as is the case now, but include the full range of trucks and other vehicles, such as boats, a group like Al Qaeda might employ in an attack.

NRC Response:
The NRC has determined that this comment is outside the scope of this rulemaking and is addressed by the Commission in 10 CFR 73.1 "Design Basis Threat".

Comment Summary:
One commenter stated that 10 CFR 73.55(e)(8)(iv) expands the purpose of the vehicle barrier beyond that specified in the Order. The commenter explained that the vehicle barrier's purpose is to prevent a vehicle bomb attack from reaching an area where it could disable equipment necessary for the safe shutdown of the plant. It is not a purpose of the vehicle barrier to prevent any type of vehicle from delivering unauthorized personnel to the proximity of the plant PA.

The commenter stated that implementation of this proposed requirement could require the installation of a "protected area" type barrier in addition to the current vehicle barrier. Further, the commenter stated that this is a significant new requirement that is not evaluated in the Regulatory Analysis. If it is not the Commission's intent to impose a new requirement, the commenter recommended the Commission delete the provision from the final rule.

NRC Response:
The Commission agrees in part. The Commission disagrees that this is a new requirement. However, the Commission revised this requirement, consistent with the pre-existing 10 CFR 73.55(c)(7), to generically address vehicle control measures as applicable to land vehicles, watercraft, trains, and other vehicles that are within the DBT as stated in 10 CFR 73.1. The final rule in 10 CFR 73.55(e)(10)(i) addresses land vehicles, and the final rule in 10 CFR 73.55(e)(10)(ii) addresses waterborne vehicles.

Comment Summary:
Another commenter stated that proposed 10 CFR 73.55(e)(8)(iv) is not performance-based (the performance-based requirement would be ensuring that the combination of the VBS and other barriers including the PA fence prevent unauthorized vehicle entry to the PA). The commenter argued that vehicle use does not need to be stopped at the VBS or prevented in proximity to the PA if the vehicles could not reach or breach the PA barrier (e.g., motorcycles between bollards).

The commenter recommended that the Commission revise the provision for consistency with the existing DBT to ensure that the combination of the VBS and other barriers including the PA

fence prevent unauthorized vehicle entry to the PA. To accomplish this, the commenter recommended that the Commission replace the phrase “beyond a vehicle barrier system” with “beyond the stand-off distance needed to effectively implement the protective strategy, maintain safe shutdown capabilities, and prevent spent fuel damage” and delete the phrase “gain proximity to a protected area or vital area, or otherwise penetrate the protected area perimeter.”

NRC Response:
The NRC agrees in part. The Commission revised this requirement, consistent with the pre-existing 10 CFR 73.55(c)(7), to generically address vehicle control measures as applicable to land vehicles, watercraft, trains, and other vehicles that are within the DBT as stated in 10 CFR 73.1. The final rule in 10 CFR 73.55(e)(10)(i) addresses land vehicles, and the final rule in 10 CFR 73.55(e)(10)(ii) addresses waterborne vehicles.

Comment Summary:
One commenter stated that the proposed 10 CFR 73.55(e)(8)(i) expands the purpose of the vehicle barrier to include control of personnel and all design basis vehicles which are beyond that specified in the Order. The commenter noted that the vehicle barrier’s purpose is to prevent a vehicle bomb attack from reaching an area where it could disable equipment necessary for the safe shutdown of the plant. It is not a purpose of the vehicle barrier to prevent any type of vehicle from delivering adversaries to the proximity of the plant. The commenter argued that existing protective strategies adequately address this situation and implementation of this requirement could require the installation of a “protected area” type barrier in addition to the current vehicle barrier which is not supported by NRC Force-on-Force inspections completed to date. Additionally, the commenter noted that the provision has no performance basis.

Therefore, the commenter recommended that the Commission revise the provision to state: “Prevent unauthorized vehicle access or proximity to any area from which the vehicle’s contents (vehicle bomb threat as discussed in the design basis threat) could disable equipment needed for safe shutdown of the plant or the personnel, equipment, or systems necessary to successfully implement the protective strategy.”

NRC Response:
The Commission agrees in part. This proposed 10 CFR 73.55(e)(8)(i) is subsumed in the final rule in 10 CFR 73.55(e)(1)(i) and (e)(10). The Commission disagrees that licensees need only to protect against the vehicle bomb. The pre-existing 10 CFR 73.55(c)(7) requires vehicle control measures to preclude vehicle proximity to VAs. Therefore, it is the Commission's expectation that vehicle control measures will include protection against any vehicle, land or water based, within the DBT, for which the licensee's site-specific analysis has identified a need to protect against.

The Commission agrees that the purpose of the VBS is to prevent a vehicle bomb attack from reaching an area where it could cause radiological sabotage and disagrees with the assumption that the licensee is not required to prevent other types of vehicles from transporting adversaries or materials to areas of the facility from which the adversary or material could disable the licensee’s capability to protect against radiological sabotage.

Comment Summary:
Another commenter stated that the phrase “proximity to” in 10 CFR 73.55(e)(8)(i) makes the proposed rule too vague. The commenter argued that it is not necessary to include this phrase

if vehicles are excluded from the areas from which unacceptable damage could occur. With this phrase, the commenter stated that the rule could be construed to include any area outside the vehicle barrier system (VBS), even when control of vehicles in the area is not required to demonstrate an effective defense against either the stand-alone or coordinated attack. Further, the comment stated that the intent of including "its personnel" also is unclear, as it is not feasible to prevent adversaries from launching a coordinated attack from anywhere outside of the VBS. The commenter recommended that the Commission delete the phrases "proximity to" and "its personnel" from the final rule.

NRC Response:
The pre-existing 10 CFR 73.55(c)(7) requires vehicle control measures to preclude vehicle proximity to VAs. The term proximity as used in the final rule is retained from the pre-existing 73.55(c)(7).

The Commission agrees that the purpose of the VBS is to prevent a vehicle bomb attack from reaching an area where it could cause radiological sabotage. However, the Commission disagrees with the assumption that the licensee is not required to prevent other types of vehicles from transporting adversaries or materials to areas of the facility from which the adversary or material could disable the licensee's capability to protect against radiological sabotage.

Comment Summary:
One commenter stated that this provision requires that licensee have land vehicles capable of preventing access that would disable personnel, equipment, or systems necessary to meet performance objectives of 10 CFR 73.55(b). Paragraph 73.55(b) requires diversity and redundancy of equipment. Thus, the commenter asked, "Must the licensee prevent land and waterborne vehicle access to all redundant sets of equipment also, or simply ensure that both sets are not disabled?"

NRC Response:
The Commission has revised the final rule to clarify that licensees are not required to protect individual pieces of equipment, which comprise defense-in-depth. The Commission's intent for the defense-in-depth requirement is so that the loss of any one component does not cause the failure of the entire physical protection program. Therefore, the licensee can lose redundant equipment provided at least one set remains capable of performing its required function.

Comment Summary:
One commenter stated that the proposed 10 CFR 73.55(e)(8)(ii) is too broad and should be re-written to define the approach routes expected to be controlled. Further, the commenter noted that, as delineated in 10 CFR 73.55(e)(8)(iii), licensees must design and install a vehicle barrier system, to include passive and active barriers, at a stand-off distance adequate to protect personnel, equipment, and systems against the DBT. Therefore, the installed vehicle barrier system, in and of itself, serves as the control of vehicle approach routes. The commenter recommended that the Commission delete this provision from the final rule.

NRC Response:
The Commission agrees in part. This proposed requirement is subsumed in the final rule in 10 CFR 73.55(e)(10). The specific measures needed to limit and control vehicles are determined by site-specific conditions. Approach routes can be controlled through the use of vehicle

controls such as vehicle barriers, channeling barriers, natural terrain, etc. the intent of which is to provide a common access path which in turn facilitates the identification of potential threats that may leave the common access path, thereby providing early detection of a possible threat.

Comment Summary:
Another commenter stated that the proposed requirement in 10 CFR 73.55(e)(8)(ii) is not performance-based. The commenter argued that the provision is not only not "critical" but utterly unnecessary to control vehicles outside the VBS and OCA in order to demonstrate an effective defense against either the stand-alone or coordinated attack. The commenter noted that the only pertinent requirement is from the February 25, 2002 Interim Compensatory Measures (ICM) Order, which is to control access by means of a vehicle checkpoint. The commenter recommended that the Commission either delete this provision from the final rule or make it consistent with the requirements outlined in the February 25, 2002 ICM Order.

NRC Response:
The Commission disagrees. The specific measures needed to limit and control vehicles are determined by site-specific conditions. Approach routes can be controlled through the use of vehicle controls such as vehicle barriers, channeling barriers, natural terrain, etc. the intent of which is to provide a common access path which in turn facilitates the identification of potential threats that may leave the common access path, thereby providing early detection of a possible threat.

Comment Summary:
Another commenter stated that having guards at the entrance to Three Mile Island would be consistent with the proposed rule regarding main entrance and alternate routes. Guards at the entrance would provide both a visual deterrent to attackers by signaling multiple layers of defense, and also would provide a level of observation that cannot be provided by security cameras alone.

In order to preserve a viable response plan for offsite responders, the bridges to Three Mile Island, which are currently vulnerable to attack, must be protected. The current SCP calls for emergency responders to be transported to the island by watercraft or aircraft, but does not take into account weather conditions where these options are not viable. The commenter also stated that members of the public have been detained for crossing an inconspicuous blue line near the north entrance to Three Mile Island, when there is no sign or indication that crossing this line is not permitted.

NRC Response:
This suggested requirement is site-specific and is not within the scope of this rulemaking. Where such site-specific measures are determined necessary through site-specific analysis for protection against the design basis threat of radiological sabotage, the performance-based requirements of this rule would require that such measures be taken. In addition, the Commission has determined that local roads and bridges that are not subject to licensee control are equally important and vulnerable to attack with regards to the capability of offsite support agencies to respond to any site. The requirement to control vehicles once onsite is generic to protection against the design basis threat of radiological sabotage and, therefore, is intended to be flexible to allow each licensee to apply the measures as necessary to meet the performance objective and requirements of 10 CFR 73.55(b).

Comment Summary:
Multiple commenters stated that they would like to see armed guards both at their present location and at the entrance to Three Mile Island off Route 441.

NRC Response:
As stated above, this suggested requirement is site-specific and is not within the scope of this rulemaking.

Comment Summary:
One commenter stated that having guards on the east shore off of Three Mile Island is not worth the trouble because it could raise many more false alarms. It would be clear that if someone tried to cross one of the bridges that it would not be a false alarm. The commenter stated that having guards off the island would also draw more attention to the presence of the nuclear power plant.

NRC Response:
As stated above, this suggested requirement is site-specific and is not within the scope of this rulemaking.

Comment Summary:
One commenter stated that 10 CFR 73.55(e)(8)(iii) expands the purpose of the vehicle barrier to include all aspects of the DBT which is beyond the Order requirements. The commenter recommended that the Commission revise the provision by replacing the phrase “and systems against the design basis threat” with “vehicle bomb threat as discussed in the design basis threat.”

NRC Response:
The Commission agrees in part. The NRC has revised the final rule to specifically address the “land vehicle bomb”. The Commission's expectation is that licensees will protect the personnel, systems, and equipment needed for safe shutdown and to implement the protective strategy, against the effects of the vehicle bomb.

Comment Summary:
Another commenter stated that 10 CFR 73.55(e)(8)(iii) exceeds the DBT requirement for standoff from the personnel, equipment and systems required for protection of the reactor, spent fuel, and implementing the protective strategy. The commenter argued that the provision unnecessarily requires protection for all personnel, equipment and systems, even those that are not required to be protected to prevent radiological sabotage or spent fuel sabotage.

Also, the commenter noted that implementation would require a new VBS to provide the additional standoff, which is not feasible within the existing OCA at many facilities. The commenter suggested that the NRC revise the provision to limit it to the personnel, equipment and systems required for protection of the reactor, spent fuel, and implementing the protective strategy, consistent with the existing DBT. To do this, the commenter suggested that the NRC replace the phrase “against the design basis threat” with “needed to implement the protective strategy, maintain safe shutdown capabilities, and prevent spent fuel damage by the design basis threat.”

NRC Response:

The NRC has revised the final rule to clarify that licensees will protect the personnel, systems, and equipment needed for prevention of significant core damage and spent fuel sabotage against the effects of the vehicle bomb.

Comment Summary:
One commenter noted that 10 CFR 73.55(e)(8)(iii) establishes the standoff distance to accomplish 10 CFR 73.55(e)(8)(i). The commenter argued that the requirement does not specify personnel (administrative, training, response, operational, etc.) and does not refer to whether the redundancy standard fits here. Thus, the commenter asked: Is the standoff distance required to protect all personnel?

NRC Response:
The Commission does not identify the specific personnel, systems, and equipment that require protection because such a determination is site-specific and must be identified to satisfy 10 CFR 73.55(b)(4). The Commission has revised the final rule text to clarify the scope of this requirement.

Comment Summary:
One commenter stated that 10 CFR 73.55(e)(8)(v) is unclear concerning the extent of periodic checking needed, particularly whether loss of power testing must be included. The commenter recommended that the Commission clarify the provision or SOC regarding whether or not the periodic checks must include loss of power testing.

NRC Response:
The Commission disagrees. The specific periodicity for testing is system-specific. The Commission's expectation is that this periodicity will be of appropriate frequency as to ensure operability of the equipment. The licensee must determine if loss of power testing is appropriate for the equipment used to ensure that it is operable.

Comment Summary:
Another commenter supported the requirement for backup electricity or for a manual closure capability of vehicle barriers, and periodic tests of their operability. This was one of the lessons learned at Three Mile Island on September 11, 2001, when guards could not close the entrance barrier because there was no electricity to power it shut.

NRC Response:
No response needed.

Comment Summary:
One commenter stated that 10 CFR 73.55(e)(8)(vi) could be broadly interpreted to mean “continual” surveillance and observation requiring the use of closed-circuit television or other continuous means. The commenter noted that at the March 9, 2007, public meeting, the NRC indicated that they believe this proposed requirement is already implemented through the Orders and is already part of the site plans. The commenter did not agree and recommended that the Commission revise the provision to state: “Provide periodic surveillance and observation of installed vehicle barriers and barrier systems to detect tampering and to ensure the integrity of the vehicle barrier and barrier system.”

NRC Response:

The Commission agrees in part. The Commission has revised the final rule text to include the word “periodic” to clarify that this requirement is not continuous and the words "tampering" and "degradation" to clarify the focus of the periodic surveillance. The Commission’s expectation is that the licensee will identify adverse conditions that would prevent the VBS from performing its function before the condition can be exploited.

Comment Summary:
Another commenter stated that the proposed 10 CFR 73.55(e)(8)(vi) is not performance-based. Also, the commenter stated that the provision could be construed to require continuous camera observation of all portions of the VBS, which is beyond what is currently required for the DBT. Further, the commenter stated that the undefined term, “unauthorized activities,” has a different meaning in this subsection than in all other uses throughout proposed changes to 10 CFR 73.55 and should be deleted. The commenter stated that the SOC implies that the meaning of “unauthorized activities” in this section is “tampering.” If so, the commenter recommended that the Commission replace the phrase “to detect unauthorized activities” with “to detect tampering.” The commenter also recommended that the NRC should revise the rule or SOC to require a level and frequency of inspection for vehicle barriers commensurate with the mass and robustness of the barrier, and consistent with the DBT.

NRC Response:
The Commission agrees in part. The Commission has revised the final rule text to include the word “periodic” to clarify that this requirement is not continuous and has replaced the phrase “unauthorized activities" with the term "tampering". Additionally, the Commission disagrees that the level and frequency of inspection for vehicle barriers must be commensurate with the mass and robustness of the barrier. The final rule requires that vehicle barriers (regardless of construction) must be inspected at a level and frequency adequate to detect indications of tampering and degradation, and ensure that the barrier is able to satisfy its function. The rationale for this performance-based requirement is that site-specific conditions effect the necessary periodicity. For example, sites that are located near the ocean may need to account for the effects that salt air has on metal which could necessitate more frequent inspections than would be needed at sites located in a dry, desert environment.

Comment Summary:
One commenter supported requirements that licensees provide protection from watercraft. The commenter stated that the only way that this can be realistically handled is with water craft barriers, which can delay entry into restricted waterways. Buoy lines are not sufficient. The commenter stated that monitoring is not sufficient. The commenter recognized the hardship this places on licensees which would have to replace floating barrier systems damaged by ice and noted that it may be cost-effective to deploy permanent barrier systems.

NRC Response:
The Commission agrees in part. The Commission disagrees that the only way to protect waterway approaches is through the use of physical barriers. The Commission has determined that the specific protective measures required to satisfy this requirement are site-specific and are predicated upon maintaining the capability to prevent significant core damage and spent fuel sabotage and implementation of the site protective strategy. The Commission agrees that, in some cases, water craft barriers may be the preferred measure however, at other sites, different measures may be most appropriate and this flexibility is needed to adequately account

for site-specific conditions.

Comment Summary:
Another commenter suggested some options for security of waterways: secure the perimeter with floating water barriers, require a net across the mouth of the intake canal to prevent explosives being sent up, such as was recommended and offered to Millstone nuclear power station in Connecticut by the Department of Homeland Security, and increase surveillance.

NRC Response:
The Commission agrees in part. As stated above, the Commission agrees that the suggested options could be viable options given the appropriate site-specific conditions. However, such detailed measures are "options" and are not appropriate for this rulemaking.

Comment Summary:
One commenter stated that waterborne defenses of nuclear plants adjacent to navigable waterways must be significantly enhanced. The commenter stated that facilities must either be engineered to withstand damage from a waterborne attack or suited with physical barriers that prevent entry to the plant and/or critical cooling intake equipment.

NRC Response:
The Commission agrees in part. The measures needed at any one site are site-specific and they consider the effects stated by this commenter.

Comment Summary:
Another commenter stated that proposed 10 CFR 73.55(e) attempts to address the threat of a waterborne vehicle attack by requiring licensees to restrict approaches to the plant by water, and to "install waterborne vehicle control measures, where applicable." The commenter noted that this degree of regulatory flexibility is in sharp contrast to the vehicle barrier requirements found in 10 CFR 73.55(e)(8)(iii), which state that the licensee must "design and install a vehicle barrier system, to include active and passive barriers, at a stand-off distance adequate to protect personnel, equipment, and systems against the design basis threat."

The commenter stated that at the March 9, 2007, public meeting, the NRC was asked about this difference in oversight, and responded that local and state jurisdiction of waterways made it less likely that the NRC could make the same requirement for waterborne barriers. Therefore, the NRC recommended a higher level of regulatory flexibility to accord licensees more latitude to comply with this new requirement.

Using an Indian Point example, the commenter noted that Entergy has installed floating buoys to delineate a 300-yard exclusion zone in front of the plant -- clearly the licensee has been accorded a certain level of control over this section of the Hudson River, from the buoy perimeter inward to the bulkhead of the plant property. The commenter asked: Why, then, is the NRC reluctant to require that Entergy replace the buoys with a system of floating, waterborne barriers that would deter or prevent a range of water-based attacks?

NRC Response:
The Commission disagrees that a different protection standard applies for protection against waterborne vehicles. The final rule requires that each licensee provide protection against the design basis threat vehicle bomb from both land and waterway approaches. The Commission acknowledges that there are significant differences between land vehicles and watercraft and

the ability of each to continue its forward momentum. Specifically, with respect to a waterborne vehicle, the shoreline or land itself may act as a watercraft barrier and can provide sufficient standoff distance. Therefore, depending on site-specific conditions, there may be no need to require a watercraft barrier. The same applies to land vehicle barriers. Natural terrain features can be used to as part of the VBS where site-specific conditions support this use. Nonetheless, the requirement to protect against vehicle bombs, applies to both land and waterway approaches.

Comment Summary:
One commenter suggested that the Commission combine 10 CFR 73.55(e)(9)(i) and 73.55(e)(9)(iv) because, in many cases, assistance will be required from outside agencies. The commenter recommended that the Commission revise the provision to state: "The licensee shall establish measures to prevent unauthorized waterborne access or proximity to any area from which a waterborne vehicle, its personnel, or its contents could disable equipment needed for safe shutdown of the plant or the personnel, equipment, or systems necessary to successfully implement the protective strategy."

NRC Response:
The Commission agrees in part. This proposed requirement is subsumed in the final rule in 10 CFR 73.55(e)(10). However, the Commission disagrees with the suggested rule text change.

Comment Summary:
One commenter stated that 10 CFR 73.55(e)(9)(i) requires that licensee have the capability of preventing access that would disable personnel, equipment, or systems necessary to meet performance objectives of 10 CFR 73.55(b). Paragraph 73.55(b) requires diversity and redundancy of equipment. Thus, the commenter asked: Must the licensee prevent land and waterborne vehicle access to all redundant sets of equipment also, or simply ensure that both sets are not disabled?

NRC Response:
Licensees are required to maintain the capability to prevent significant core damage and spent fuel sabotage which may in turn necessitate the use of equipment. Therefore, the licensee is required to protect (remain operable to perform intended function) a minimum of one (1) group of equipment required to prevent significant core damage and spent fuel sabotage, but is not required to protect equipment that is redundant to the one (1) protected group.

Comment Summary:
Another commenter stated that the proposed requirement for controlling waterway approach routes is not performance-based and it is unnecessary to control vehicles outside the OCA in order to demonstrate an effective defense against either the stand-alone or coordinated attack. In addition, the commenter stated that the phrase "proximity to" makes the proposed rule too vague, and is not necessary if vehicles are excluded from the areas from which unacceptable damage could occur. The commenter noted that this phrase could be construed to include any area outside the OCA, even when control of waterborne vehicles in the area is not required to demonstrate an effective defense against either the stand-alone or coordinated attack. The commenter stated that the intent of including "its personnel" also is unclear, as it is not feasible to prevent adversaries from launching a coordinated attack from anywhere outside of the OCA.

The commenter stated that the NRC should delete the proposed requirement for controlling

waterway approach routes, add a qualifier that allows the exclusion for those facilities not impacted by waterborne vehicles, and delete the phrases “proximity to” and “its personnel” from this provision. Additionally, the commenter recommended that the Commission replace the phrase “as described in paragraph (b) of this section” with “as described in the Commission-approved security plan.”

NRC Response:
The Commission disagrees. The term “proximity” was used consistent with the pre-existing 10 CFR 73.55(c)(7). The Commission disagrees with the suggested rule text changes.

Comment Summary:
A commenter stated that the final rule must address the risk of waterborne attacks by requiring an equivalent level of protection for both water-based and land-based vehicle threats. The commenter stated that the Commission must remove the “where applicable” language of 10 CFR 73.55(e)(9)(ii), and additional language needs to be added to clarify the requirement for “waterborne vehicle control measures,” so that they also “protect personnel, equipment and systems against the design basis threat.”

NRC Response:
The Commission agrees in part. The NRC has revised the final rule in 10 CFR 73.55(e)(10)(i) and (ii) to clarify the performance-criteria for both land and water based vehicles. Licensees are required to protect against the adverse effects that a vehicle bomb could have on their capability to prevent significant core damage and spent fuel sabotage to include the capability to implement the site protective strategy.

The NRC disagrees with the suggestion to require waterborne control measures at all sites without consideration to site-specific conditions. Each site must design the physical protection program to account for site specific conditions. The Commission revised the final rule to clarify that waterborne vehicle control measures are determined through site-specific analysis and that where the analysis has identified a need, measures must be taken to account for the identified condition. The phrase “where applicable” is revised to "as necessary” in the final rule.

Comment Summary:
A commenter recommended that the Commission combine 10 CFR 73.55(e)(9)(iv) with 10 CFR 73.55(e)(9)(i).

NRC Response:
The Commission disagrees. The Commission concluded that this requirement is appropriate as a stand-alone requirement. The requirement to “coordinate” is intended to apply where a licensee has determined that waterway physical protection measures are prudent, but the licensee does not own or have rights to that waterway. In such cases the licensee must request authorization from the governmental entity having jurisdiction or ownership of the affected waterway.

Comment Summary:
One commenter stated that 10 CFR 73.55(e)(9)(iii) is more stringent than the requirements contained in the current regulations and Orders. The commenter argued that the need to “monitor waterway approaches and adjacent areas to ensure early detection, assessment, and response to unauthorized activity or proximity” is protective strategy-dependent. The commenter recommended that the Commission revise the provision to state: “As needed to

successfully implement the protective strategy, the licensee shall monitor waterway approaches and adjacent areas to ensure response to unauthorized intruders is provided."

NRC Response:
The Commission agrees in part. The Commission has revised the final rule to clarify that surveillance and observation of waterway approaches is site-specific and must ensure the effective implementation of the site protective strategy.

Comment Summary:
Another commenter stated that the proposed 10 CFR 73.55(e)(9)(iii) is not applicable to all facilities. The commenter stated that, similar to the proposed rule wording in the new 10 CFR 73.55(e)(9)(ii), the Commission should add a qualifier that allows the exclusion for those facilities not impacted by waterborne vehicles. Therefore, the commenter suggested that the NRC add the phrase "as applicable" after "adjacent areas."

NRC Response:
The Commission agrees in part. The Commission agrees that this requirement is not applicable to sites and must be applied in accordance with site-specific analysis required by the final rule 73.55(b)(4). However, the NRC disagrees with the suggested rule text change.

Comment Summary:
One commenter at the November 15, 2006, public meeting asked for a clarification of the relationship between target sets and vital equipment. The NRC responded that the difference between vital equipment and target sets would be that target sets include vital equipment, but vital equipment does not always contain everything that may be part of a target set. Target sets would be the combination of equipment, systems, even personnel, that would need to be disabled or destroyed in order to cause a problem. So, the commenter deduced that vital equipment would be part of the target set, but the target set, itself, may include additional things to it that would also be protected.

The NRC explained that requiring licensees to protect target sets protects those systems, personnel, or equipment that are necessary for a safe shutdown. The NRC concluded that vital equipment is related to safe shutdown and target sets are related to release. Another commenter at the November 29, 2006, public meeting asked if a licensee can lose vital equipment without either losing the ability for safe shutdown or losing a target set. The NRC responded that yes, it is possible.

NRC Response:
Vital equipment is related to safe shutdown while target sets are related to release of radioactive
material (or significant core damage and spent fuel sabotage). Therefore, the physical protection program design criteria in 10 CFR 73.55(b) focuses on prevention of significant core damage and spent fuel sabotage and the ability to effectively implement the protective strategy as performance-criteria resulting from the protection of target sets.

Comment Summary:
A commenter at the November 15, 2006 public meeting asked if a NUREG from the 1990s is a good source for defining vital equipment.

NRC Response:
NRC published information remains acceptable unless otherwise stated by the Commission.

Comment Summary:
One commenter stated that there must be a requirement to identify certain bridges as “targets.” The commenter stated that this should include access bridges, which if lost, would adversely affect or even negate the offsite responders’ capabilities. The commenter argued that since the Commission is requiring licensees to “identify target sets” and “to include analyses and methodologies used to determine and group the target set equipment or elements,” and because numerous emergency scenarios rely upon offsite responders as one of those “elements” to prevent “significant core damage or spent fuel sabotage,” bridges must be identified as targets.

NRC Response:
The Commission disagrees. This comment is sufficiently addressed through Commission regulations pertaining to protection against the DBT. This commenter suggests that bridges leading to a facility must be protected to ensure an offsite response is able to reach the facility. Upon consideration, the Commission has determined that the suggested protection for bridges is impractical and unnecessary because the tactic of destroying bridges also applies equally to all other public road surfaces and bridges between the facility and the location from which the offsite response will originate. Therefore, the Commission concluded that the suggested requirement constitutes an unreasonable regulatory burden that is outside the scope of this rulemaking.

Comment Summary:
Another commenter stated that proposed 10 CFR 73.55(f)(1) would require licensees to document their target set development process in “site procedures,” but other site documents (e.g., engineering calculations versus site procedures) were utilized to document this process. The commenter argued that it is not necessary to limit the documentation to site procedures, provided that the methodology is documented and maintained consistent with the site configuration control process. The commenter recommended that the Commission revise this provision to require the methodology to be documented and maintained consistent with the site configuration control process. The commenter recommended that the Commission delete “in site procedures” from the provision.

NRC Response:
The Commission agrees. The requirement to document this process “in site procedures” has been deleted from final rule text to clarify that it is acceptable for the licensee to reference rather than include, supporting documentation. This documentation must be maintained in accordance with the final rule 10 CFR 73.55(q) "Records" and made available to the NRC upon request and in a timely manner needed to support any NRC inquiry or inspection.

Comment Summary:
One commenter stated that 10 CFR 73.55(f)(2) is more stringent than the Orders. If retained, the commenter recommended that the Commission move the language to 10 CFR 73.55(m) so that the requirements for cyber security are listed together. Further, the commenter suggested that the Commission revise the language by adding the word “disabling” before “individual equipment.”

NRC Response:
The Commission disagrees. The focus of this requirement is on "Target Sets" and the effects that cyber attacks can have to “disable” or prevent target set equipment from performing its function. The requirements in the proposed 10 CFR 73.55(m) have been moved to a stand-alone 10 CFR 73.54 and focus on the broader cyber security program. Therefore, the Commission concluded that this requirement is appropriate to this paragraph.

Comment Summary:
Another commenter stated that 10 CFR 73.55(f)(2) only makes sense if the normal, emergency, backup, or alternate safe shutdown equipment is digitally controlled. The commenter argued that in cases where only local, manual operation of systems is credited, this requirement imposes an unnecessary burden with no value. In addition, the commenter noted that no guidance has been developed for implementing such a requirement. Lastly, the commenter noted that the NRC approved the guidance contained in NEI 03-11, “Guidance for the Preparation and Conduct of Force-on-Force Exercises,” Revision 1, dated December 2005, Chapter 4, “Target Set Development,” and the associated NRC-developed “Target Set Information Worksheet.” These documents did not require consideration of cyber attacks.

Since this was what the existing target sets are based on, the commenter said that such a new requirement, as proposed in the new 10 CFR 73.55(f)(2), would require all licensees to revise their existing target sets and associated documentation. Accordingly, the commenter recommended that the NRC delete the provision from the final rule.

NRC Response:
The Commission disagrees that this is a new requirement and has concluded that it appropriately updates Commission regulations consistent with the DBT stated in 10 CFR 73.1 which includes cyber attack capabilities. The Commission’s expectation is that licensees will ensure that the cyber capabilities attributed to the design basis threat are accounted for in the developed target sets and if necessary, each licensee will re-evaluate developed target sets to consider the affects of a cyber attack. Therefore, the Commission disagrees with the suggested rule text change.

Comment Summary:
One commenter stated that the proposed 10 CFR 73.55(f)(3) is more stringent than the Order requirements. The commenter argued that incorporating target set equipment or elements that are not contained within a protected or vital area or otherwise, into the security plan, will limit flexibility in responding to the changing threat environment in a timely manner since changes would require prior NRC review and approval. Thus, the commenter recommended that the Commission delete this requirement from the final rule.

NRC Response:
The Commission agrees in part. The Commission agrees that listing target-set equipment in the NRC-approved security plan is an unnecessary regulatory burden, as it would require plan changes whenever site-conditions change. Therefore, the Commission has revised the final rule to require that these target set elements be identified through the documentation required in 10 CFR 73.55(f)(1), the product of which is a listing of target sets that can be modified without prior Commission approval. Given this revision, the Commission disagrees with the recommendation to delete this requirement.

Comment Summary:

Another commenter noted that 10 CFR 73.55(f)(3) adds a requirement that the target set equipment outside the PA or VA must be explicitly identified in the approved security plans, and addressed by the licensee's protective strategy. The commenter stated that it is unclear what benefit, if any, inclusion of this information in security licensing and plant level documents would provide. The commenter stated that for the DBT, the specific equipment included in target sets is already identified in the target set documents and addressed by the tamper protection portion of the insider mitigation program (IMP). The commenter recommended that the Commission revise the provision to require that such equipment be explicitly identified in the target set documents and included in the tamper protection portion of the IMP.

Accordingly, the commenter recommended that the Commission replace "approved security plans and protective measures for such equipment or elements must be addressed by the licensee's protective strategy in accordance with appendix C to this part" with "licensee's target set documents and included in the tamper protection portion of the Insider Mitigation Program."

NRC Response:
The Commission agrees in part. Therefore, the Commission has revised the final rule to require that these target set elements be identified through the documentation required in 10 CFR 73.55(f)(1), the product of which is a listing of target sets that can be modified without prior Commission approval. However, the Commission disagrees that reference to the IMP is necessary because this element of the IMP is addressed in 10 CFR 73.55(f)(4).

Comment Summary:
One commenter stated that Operations already have controls in place to maintain configuration control through normal operations and surveillance and the proposed 10 CFR 73.55(f)(4) requirement should only address obvious tampering. Additionally, the commenter noted that the terms "significant core damage" and "spent fuel sabotage" are not defined terms in 10 CFR 73.2. The commenter recommended that the NRC delete the phrase "to ensure that changes to the configuration of the identified equipment and systems do not compromise the licensee's capability to prevent significant core damage and spent fuel sabotage" from the final rule.

NRC Response:
The Commission agrees in part. The Commission agrees that licensee Operations already have controls in place that may satisfy this requirement and it is the Commission's expectation that these pre-existing controls will be used. In addition, this requirement is intended to be incorporated as an element of the Insider Mitigation Program to include obvious indications of tampering. Therefore the NRC considers this to be a current requirement consistent with current licensee practices. The NRC has deleted reference to "significant core damage and spent fuel sabotage" from the final rule to clarify that the focus of this requirement is on oversight of target set equipment to ensure that the licensee's protective strategy is not adversely impacted by configuration changes to target set equipment.

Comment Summary:
Another commenter stated that 10 CFR 73.55(f)(4) is redundant to other provisions in the proposed rule (e.g., 10 CFR 73.55(i)(9) and 10 CFR 73.58). Therefore, the commenter recommended that the Commission delete proposed 10 CFR 73.55(f)(4) from the final rule.

NRC Response:
The Commission disagrees. The Commission has determined that this requirement is related to but not redundant to the referenced requirements and is necessary to establish the regulatory

framework and performance-criteria connecting oversight of target set configuration to the IMP and safety/security interface.

Comment Summary:
A commenter stated that the proposed 10 CFR 73.55(g) does not close a dangerous loophole in current search requirements for law enforcement personnel and security officers. The commenter noted that the current rule at 10 CFR 73.55(d)(1) states that, "The licensee shall control all points of personnel and vehicle access into a protected area ...." The licensee shall subject all persons except bona fide Federal, State, and local law enforcement personnel on official duty to these equipment searches upon entry to a protected area. Armed security guards who are on duty and have exited the protected area may reenter the protected area without being searched for firearms."

The commenter stated that proposed 10 CFR 73.55(g)(1) no longer specifically authorizes these exceptions to the search procedures, but would still allow them, subject to Commission review and approval. 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, as approved by the Commission.

NRC Response:
The Commission disagrees. The specific provisions addressed by this comment were retained from the pre-existing rule and remain applicable through the provisions of the final rule in 10 CFR 73.55(g)(4) and 73.55(h)(8). The Commission has determined that retention of these requirements is appropriate and consistent with NRC requirements for background checks, psychological assessments, and behavior observation (trustworthiness and reliability). It must be noted that armed security personnel are searched prior to reporting for duty and being issued a firearm. This provision simply allows armed personnel to exit the PA with their assigned weapon, to perform official duties and then re-enter without re-search for a firearm.

With respect to bona fide Federal, State, and local law enforcement personnel on official duty, they are subject to their own trustworthiness and reliability determinations which are outside the scope of this rulemaking. It is important to note that this flexibility does not relieve the licensee of its responsibility to prevent the introduction of unauthorized items or materials that would otherwise be prevented from access and only applies to those weapons or items that are "issued to designated armed personnel in the performance of "official duties".

Comment Summary:
Several commenters stated that proposed 10 CFR 73.55(g)(1)(i) is more stringent that current regulations and Order requirements.

NRC Response:
The Commission disagrees. The Commission has revised the final rule to clarify that the scope of this requirement is limited to the intended function of each access portal. The specific function is determined by each licensee based on site-specific analysis.

Comment Summary:
One commenter stated that 10 CFR 73.55(g)(1)(i) requires personnel control into the OCA; whereas, currently only vehicle control into the OCA is required. The commenter recommended

that the Commission revise this provision by deleting “any” before “applicable areas” and adding the phrase “in accordance with the Commission-approved security plans” to the end of the provision.

NRC Response:
The Commission agrees in part. The Commission has revised final rule in 10 CFR 73.55(b) and in this requirement to clarify that access controls in the OCA are based on site-specific conditions. The use of a VBS or other physical barrier in the OCA is a product of the licensee’s analysis of their site-specific conditions. The Commission disagrees with the suggested rule text change because NRC requirements are stated in the regulations, not in the licensee security plans.

Comment Summary:
Another commenter argued that 10 CFR 73.55(g)(1)(i) is ambiguous and can be interpreted broadly to apply new requirements to the OCA (e.g., vehicle barrier) that are impracticable and unnecessary. The commenter recommended that the Commission revise the existing language for PA access to include materials and add a new section to address access through the OCA vehicle barrier system. The commenter provided the following suggested language for 10 CFR 73.55(g)(1)(i): “Control all points of personnel, vehicle, and material access into the protected area established to meet the requirements of this section.” The commenter provided the following suggested language for 10 CFR 73.55(g)(1)(i)(A): “Control vehicle access, capable of transporting the design basis threat bomb, through the vehicle barrier system, established to meet the requirements of this section.”

NRC Response:
The Commission agrees in part. The Commission has revised the final rule to clarify the scope of this requirement consistent with the final rule in 10 CFR 73.55(b). The use, placement, and function of any barrier in the OCA is contingent upon the licensee's site-specific analysis and must be constructed to meet a site-specific need identified by the licensee through that analysis. Therefore, it is the licensee who determines if a barrier is necessary in the OCA to satisfy this requirement. The Commission agrees that access controls to the protected area can be independently addressed and has revised 10 CFR 73.55(g)(2) to address PA access controls.

Comment Summary:
One commenter stated that the rule (for example, in 10 CFR 73.55(g)(1)(i)) broadly imposes requirements on “any area” or “all areas” when previously it specified the specific area.

NRC Response:
The Commission disagrees. The references to "any area" and "all areas" were used generically to represent the facility areas that each licensee identifies through the site-specific analysis. For example, the licensee determines the stand-off distance needed to support the physical protection program and meet NRC requirements. This stand-off distance can be in the OCA or at the PA perimeter.

Comment Summary:
A commenter stated that proposed 10 CFR 73.55(g)(3)(i) uses the vague term “as appropriate,” and the Commission should replace this term with more performance-based criteria. The commenter recommended that that the Commission replace “as appropriate” with “as described in the Commission-approved security plans.”

NRC Response:
The Commission agrees in part. The Commission has deleted the phrase "as appropriate" and has revised the final rule to replace “as appropriate” with “consistent with the intended function." However, the NRC disagrees with the suggested rule text change.

Comment Summary:
One commenter stated that 10 CFR 73.55(g)(1)(v) is more stringent than the requirements contained in the Orders, which require surveillance capabilities and duress alarms. The commenter suggested that the Commission revise this provision to state: “Provide surveillance or duress alarms for badging processes located outside the protected area.”

NRC Response:
The Commission disagrees. This requirement, as worded, provides an appropriate performance-based requirement which allows the licensee to determine the site-specific measures needed to meet the requirement which may include the two measures specified by this comment. The Commission determined that this flexibility for licensees to apply site-specific measures is approriate. It is clear by this comment that the commenter does understand that this is a pre-existing requirement (i.e., not more stringent) and that the use of surveillance and duress alarms can satisfy this requirement.

Comment Summary:
Another commenter stated that the proposed 10 CFR 73.55(g)(1)(v) does not encompass current industry guidance. The commenter noted that the actual ICM guidance for Item B.4.h, states, in part, “If the badging area is outside the protected area, develop a means to avoid unauthorized bypass of the badging process or install duress capability or surveillance capability....” This commenter recommended that the Commission revise the provision to state: “Provide a means to avoid unauthorized bypass of access control equipment located outside the protected area.”

NRC Response:
The Commission disagrees. This requirement, as worded, provides a performance-based requirement which allows the licensee to determine the site-specific measures needed to meet the requirement. The NRC has concluded that the commenter clearly recognizes that this is a pre-existing requirement to which the referenced guidance applies.

Comment Summary:
One commenter noted that 10 CFR 73.55(g)(1)(iii) would require licensees to limit unescorted access to the PA during non-emergency conditions. The commenter stated that licensees currently limit unescorted access to VA during non-emergency conditions to individuals who require access in order to perform their duties. Also, many licensees grant unescorted access to the PA (with no VA access) to workers who do not frequently enter the PA, but who may have the possibility of needing access at some undefined time in the future. In addition, the commenter noted that having certain site workers limited to unescorted PA access affords their placement into the licensee’s behavior observation and Fitness for Duty or critical group programs should those workers be performing critical work even though they do not have a job-related need to access the PA. Therefore, the commenter recommended that the Commission revise this provision by replacing the phrase “limit unescorted access to the protected area and vital areas” with “limit vital area unescorted access”.

NRC Response:
The Commission disagrees that this requirement places any new or unacceptable limits on licensee employees or contractors, nor does it require licensee process changes for unescorted PA or VA access. This requirement is a fundamental program requirement intended to limit unescorted access to only those individuals who require access to perform duties. The licensee is responsible to determine who requires unescorted access and what duties are assigned to them whether those duties require daily or intermittent access. Personnel who require intermittent access are not limited by this requirement but are limited only by their assigned duties. Personnel, who do not have duties to perform, must not be granted unescorted access.

Comment Summary:
A commenter stated that 10 CFR 73.55(g)(1)(iv) is more stringent than the current requirements and Orders. As written, the commenter argued that the proposed language is ambiguous and can be interpreted broadly. For example, the commenter asked: What is the meaning of the terms “monitor,” “integrity,” and “access control system?” The commenter concluded that 10 CFR 50 Appendix B requires adequate quality controls for licensees; thus, the Commission should delete this provision.

NRC Response:
The Commission agrees in part. The Commission has concluded that this requirement is sufficiently addressed by the final rule in 10 CFR 73.55(g)(1)(i)(C) and therefore, has been deleted. The Commission's expectation is that the licensee will ensure that all access controls are working as intended and have not been compromised such that no person, vehicle, or material is able to gain unauthorized access beyond a barrier.

Comment Summary:
Two commenters stated that 10 CFR 73.55(g)(2) appears to expand the current requirements for the PA into the OCA without sufficient clarification of the performance measures, and that the results of the NRC Force-on-Force inspections do not support expanding these requirements.

NRC Response:
The Commission disagrees. The proposed rule attempted to address access controls generically with specific implementing differences between OCA and PA being described in the approved security plans. However, based on comments, the final rule is revised to prescriptively specify requirements for OCA and PA individually. This requirement is revised to address access to the PA only, and is revised to delete reference to the NRC-approved security plans which was intended to reflect the current licensee practice of describing the site-specific OCA vehicle search process in the security plans.

Comment Summary:
Further, one commenter stated that the performance measures for access controls in the OCA should be related solely to ensuring the effective implementation of the protective strategy, and 10 CFR 73.55(g)(2) should only apply to access to the PA. The commenter recommended that the Commission clarify this provision by replacing the phrase “an access control point” with “a protected area access control point.”

NRC Response:
The Commission agrees in part. The Commission agrees that access controls in the OCA must support the effective implementation of the protective strategy, however, the primary focus of

security measures in the OCA is on ensuring the effectiveness of the physical protection program of which the protective strategy is a component. Therefore, access controls in the OCA must support the effective implementation of the physical protection program and not be limited to only the protective strategy.

Comment Summary:
The same commenter noted that 10 CFR 73.55(g)(2)(i) and (g)(2)(ii) have requirements that are not required for the OCA per current regulations and Orders.

NRC Response:
The Commission agrees in part. The Commission has revised the final rule text to limit these requirements to only PA access. However, consistent with the proposed rule and current licensee practice, the Commission intended to apply these proposed requirements generically with the licensee specifying the implementing differences between OCA and PA in their security plans.

Comment Summary:
It is also noted that 10 CFR 73.55(g)(2)(iv) is not required for the OCA per current regulations and Orders, and that the requirement to check the industry database should be relocated to 10 CFR 73.56 for unescorted access and to 10 CFR 73.55(g)(7)(i) of this section for escorted access.

NRC Response:
The Commission agrees in part. The Commission agrees that this proposed requirement is PA specific and has revised the final rule to limit it to PA access only. However, the NRC disagrees that this requirement should be relocated to 10 CFR 73.56 and has retained it in the final rule 73.55(g)(2)(iii).

Comment Summary:
For 10 CFR 73.55(g)(2)(iii), it is noted that the contents are not required for the OCA per current regulations and Orders other than in relation to the DBT vehicle bomb.

NRC Response:
The Commission agrees in part. Consistent with the final rule in 10 CFR 73.55(b) the licensee must protect against all capabilities of the DBT that can endanger the public health and safety. It is the responsibility of the licensee to identify the facility areas from which the DBT can accomplish this and protect against it. It is evident by this comment that the commenter understands that this requirement is applicable to the OCA regarding the current use of a vehicle barrier in the OCA at some sites.

Comment Summary:
One commenter noted that the use of the word “qualified” in proposed 10 CFR 73.55(g)(5)(ii) is problematic because it could unnecessarily require maintenance of “qualification cards.” Thus, the commenter recommended that the Commission delete the term “qualified” from the provision.

NRC Response:
The Commission agrees. The Commission has revised final rule text to delete the term qualified to avoid unintended record keeping and has added reference to the escort

requirements addressed in 10 CFR 73.55(g)(8) for consistency.

Comment Summary:
Another commenter expressed dismay that the NRC proposed to “loosen” the requirement for armed security for all vehicles inside a nuclear power plant's protected or vital areas unless the vehicle is specially designated for use in such areas. The commenter further stated that the provision provides no explanation for the change to this requirement, particularly given that there appears to have been no change in the threat environment that might warrant this loosening of security.

NRC Response:
The Commission disagrees that this requirement loosens the requirement for armed security for all vehicles inside the PA. The current requirement in 10 CFR 73.55(d)(4) does not require armed escort for all vehicles, but rather requires that the escort be a member of the security organization, who may be an unarmed watchman. The Commission agrees that the proposed rule did not clearly state the rationale for changes to this requirement. The Commission determined that the requirements for access authorization, search requirements, controls once inside the PA, and the escort standards specified by the final rule in 10 CFR 73.55(g)(8), provide a sufficient basis to allow the licensee the flexibility to use non-security personnel for this function.

Vehicle operators must be authorized unescorted access to the PA or must be escorted by a person granted unescorted access who can call for assistance if needed. Further, consistent with the pre-existing requirement for "designated" vehicles, all vehicles in the PA must have a need for access. The Commission has determined that simply designating a vehicle for use inside the PA adds little value and is, therefore, no longer necessary.

Comment Summary:
Another commenter sought clarification of what type of equipment is intended in proposed 10 CFR 73.55(g)(5)(ii).

NRC Response:
The revised 10 CFR 73.55(g)(8) specifies escort standards and has deleted reference to equipment. The term "equipment was intended to be generic and could include anything needed to perform escort duties, such as radio.

Comment Summary:
One commenter stated that use of the term “disabled” in the proposed 10 CFR 73.55(g)(5)(iii) could be interpreted to mean more than removing the keys from a vehicle. Thus, the commenter recommended that the Commission replace “disabled” with “placed in a condition such that the vehicle would not be in a ready-to-use configuration.”

NRC Response:
The Commission agrees in part. The final rule is revised to specify that keys must be removed or the vehicle must “disabled”. The term disabled is intended to be flexible to allow each licensee to determine the best methodology for their site subject to NRC inspection.

Comment Summary:
One commenter stated that the Commission should better define the term “hazardous materials” in the proposed 10 CFR 73.55(g)(5)(iv) in accordance with current guidance to clarify the performance criteria. Also, the commenter stated that the Commission should add the phrase “or driven by personnel with unescorted access” to the end of the proposed text, which would provide adequate control of these vehicles to prevent unauthorized use to prevent effective implementation of the protective strategy.

NRC Response:
The Commission disagrees with the suggested change to the rule text because it is not consistent with current Commission expectations. Because hazardous materials pose a unique threat to a facility, vehicles carrying hazardous materials inside the PA must be escorted by armed security personnel only. The Commission disagrees that hazardous materials should be defined by this rulemaking to be consistent with guidance. Guidane is written to provide an acceptable method to meet requirements. As stated, hazardous materials are described in current guidance.

Comment Summary:
A commenter stated that the NRC should delete “lists” from this provision and replace it with “approval.” The commenter argued that doing so would allow several means of access control based on authorized approval.

NRC Response:
The Commission disagrees. This requirement is retained from the pre-existing requirement for vital area access to be controlled by an access authorization list.

Comment Summary:
One commenter stated that 10 CFR 73.55(g)(1)(vii) is more stringent than current requirements or Orders. The commenter stated that the procedures for implementing the two-person rule should address the controls required and the term “specific threat” appears to be an expansion of the current requirement to implement the two-person rule. The commenter recommended that the Commission revise the provision to state: “In response to a site specific credible threat, as defined by the Commission, implement a two-person (line-of-sight) rule for all personnel in vital areas.”

NRC Response:
The Commission agrees. The final rule is revised to include the term "site-specific" and “credible.” Also, the proposed requirement to verify that the two person rule is met when a vital area is accessed is deleted because such a requirement constitutes a requirement to verify compliance with this requirement. Compliance is already required, and therefore, this statement is not needed.

Comment Summary:
Another commenter stated that proposed 10 CFR 73.55(g)(1)(vii) implements requirements that are more stringent than the NRC ICM Order, dated February 25, 2002. The commenter noted that the NRC Order required implementation of the two-person rule only for a “credible insider threat,” but the proposed rule requires this for any security threat. Therefore, the commenter recommended that the NRC revise the provision by replacing the phrase “specific threat and security information” with “a site-specific credible threat”

NRC Response:
The Commission agrees. As stated above, the Commission revised the final rule to include the term "site-specific" and “credible.”

Comment Summary:
One commenter argued that proposed 10 CFR 73.55(g)(4)(i) is very broad and could conceivably allow the licensee to drop all access controls in an emergency, while limiting access to authorized individuals. The commenter asked: “Is there a phrase missing here, perhaps ‘without compromising the intended function of the access control’ or ‘including posting of security officers to monitor personnel access?’” The commenter noted that some detail is provided in the proposed 10 CFR 73.55(g)(4)(ii), but that section should at least be referenced here.”

NRC Response:
The Commission disagrees. It is important that licensees are not exempt from access control requirements during an emergency. The scope of this requirement is further addressed in 10 CFR 73.55(g)(5)(ii). The Commission disagrees that this requirement, as written, could allow a licensee to drop all access controls in an emergency. Even under emergency conditions, the licensee is responsible to deny access to persons who are not authorized (do not have a job related need) for access. This performance-criteria is applicable at all times.

Comment Summary:
One commenter noted that during a crisis event there is the possibility that terrorists could infiltrate a nuclear facility by posing as first responders, especially in firefighter uniforms, which would allow terrorists increased access to a facility to carry out even more destructive activities.

NRC Response:
The Commission disagrees. Licensees are not exempt from access control requirements during an emergency. Licensees are required to maintain the capability to protect against the DBT at all times which also includes emergency conditions.

Comment Summary:
Another commenter referenced the proposed 10 CFR 73.55(g)(4)(ii)(B) and requested clarification of the word “authorized.” The commenter asked if the term means that access that would be unauthorized under non-emergency situations, or unauthorized even under the more lax conditions of an emergency.

NRC Response:
The Commission determined that the correct reference for this comment is 10 CFR 73.55(g)(4)(ii)(A) not (B) as indicated in the comment. The term “authorized” as used in the final rule 73.55(g)(5)(ii) refers to emergency personnel. The licensee determines which personnel are authorized during an emergency. Under non-emergency conditions, such personnel do not posses a job related need for prompt access. Under non-emergency conditions such personnel may be processed a visitor as required by the final rule in 10 CFR 73.55(g)(7).

Comment Summary:
Another commenter recommended that the Commission replace the terms “significant core damage” and “spent fuel sabotage” with the term “radiological sabotage” because “radiological sabotage” is a defined term in 10 CFR 73.2 and the other terms are not.

NRC Response:
The Commission disagrees. The NRC determined that this requirement is sufficiently addressed by 10 CFR 73.55(b)(3) and, therefore, has deleted this proposed requirement from the final rule.

Comment Summary:
One commenter stated that 10 CFR 73.55(g)(4)(iii) is more stringent than current regulations and Orders.

NRC Response:
The Commission disagrees. However, the Commission determined that this requirement is sufficiently addressed by 10 CFR 73.55(b)(11) and, therefore, has deleted this proposed requirement from the final rule.

Comment Summary:
One commenter stated that proposed 10 CFR 73.55(g)(6)(ii), in conjunction with proposed 10 CFR 73.55(g)(6)(ii)(A), imply that "passwords" are considered access control devices, which must be controlled and accounted and only issued to individuals who require unescorted access to perform official duties and responsibilities. The commenter noted that this is a new interpretation of the current 10 CFR 73.55(d)(8) requirements and will necessitate the use of integrated directory management systems, which will add to the complexity and cost of new and existing computer systems.

The commenter stated that this type of account management system is not common for most process control vendors and several years may be necessary for vendors to incorporate this functionality into their systems. The commenter concluded that it is not clear if this applies only to access control computers or to nuclear significant computers located in VAs that allow remote access. Therefore, the commenter recommended that the Commission delete the term "passwords" from the provision.

NRC Response:
The Commission disagrees. The Commission has determined that passwords act the same as keys to allow the holder access to the information or systems/equipment that must be protected. The Commission agrees that there are differences in the type of media used and therefore differences in "how" these access control devices are controlled and accounted for but disagrees that this requirement encompasses any more than the commonly used and accepted standard key and lock and/or password control methodologies currently in use for each media type.

Consistent with pre-existing requirements for key, lock, and combination controls, the Commission's expectation is that licensees will ensure that passwords are issued only to those individuals who require access, and that the licensee implements a methodology to ensure passwords are not compromised, are changed consistent with accepted professional standards, and are disabled when access is no longer needed.

Comment Summary:
Two commenters stated that the proposed 10 CFR 73.55(g)(6)(ii) co-mingles the requirements for passwords with keys, locks, and combinations, which can lead to confusion and result in a broad interpretation of the requirements and cause unintended consequences.

NRC Response:
The Commission disagrees. This requirement does not encompasses any more than the commonly used and accepted standard key and lock and/or password control methodologies currently in use.

Comment Summary:
One commenter recommended that the Commission should address passwords comprehensively in one single section in this rule. The commenter also stated that accounting for passwords defeats the purpose of having passwords, and it is possible to account for individuals that are provided passwords(addressed in proposed 10 CFR 73.55(g)(6)(ii)(B)). This commenter concluded that long standing information technology processes in place to manage privileged user accounts should be employed to manage passwords.

NRC Response:
The Commission agrees with the commenter's conclusion. Consistent with pre-existing requirements for key, lock, and combination controls, the Commission's expectation is that licensees will ensure that passwords are issued only to those individuals who require access, and that the licensee implements a methodology to ensure passwords are not compromised, are changed consistent with accepted professional standards, and are disabled when access is no longer needed.

However, the Commission disagrees that passwords should be addressed separately by this rulemaking and that accounting for passwords defeats the purpose of a password. Accounting for a password simply means ensuring that the person is authorized access to the items that require protection and does not mean "seeing" the password. The Commission agrees that this requirement is intended to be consistent with the long standing information technology processes currently in place to manage privileged user accounts, which should satisfy this requirement subject to NRC inspection.

Comment Summary:
A commenter, referencing proposed 10 CFR 73.55(g)(6)(ii), stated that the addition of "security systems" and "safeguards information" introduces new requirements that are more stringent than the requirements of the security Orders. The commenter argued that the terminology could be broadly interpreted as requiring controls and accountability that are unmanageable and would provide little or no benefit in preventing unauthorized access to areas, systems, or information. The commenter stated that access controls for SGI should be contained in 10 CFR 73.21.

NRC Response:
The Commission disagrees that the addition of security systems and safeguards information introduce new requirements. However, the Commission agrees that the requirement for safeguards information is more appropriate for 10 CFR 73.21 and has deleted the term "safeguards information" from the final rule.

Comment Summary:
A commenter stated that the term "Access Control" is inconsistently used throughout the proposed rule and it is not always clear if "Access Control" refers to password control, hardware, or other control methods. Thus, the commenter recommended that the Commission modify proposed 10 CFR 73.55(g)(6)(ii) to state: "Keys, locks, combinations, and passwords.

All keys and locks, and related access control devices used to control physical access to protected areas, vital areas, security systems, and safeguards information must be controlled and accounted for to reduce the probability of compromise. All passwords and combinations used to control physical access to protected areas, vital areas, security systems, and safeguards information must be controlled and modified periodically to reduce the probability of compromise."

NRC Response:
The Commission disagrees. The term "access control" has been clearly and consistently used throughout this rulemaking as a generic term with generic meaning. Access controls apply generically and equally to both physical and electronic access. This paragraph appropriately addresses generic performance-based requirements, for the "control" of all devices that can be used to gain access (physical or electronic) to areas, materials, systems, equipment, and/or information that has been determined by the licensee to require protection to meet NRC requirements.

Comment Summary:
One commenter stated that access to SGI is sometimes necessary for individuals without unescorted access to a facility because they have no need for access to the facility to perform their responsibilities. The commenter stated that proposed 10 CFR 73.55(g)(6)(ii)(A) does not apply to passwords, and passwords are not considered a part of "access control equipment." The commenter requested that the Commission clarify physical access controls as opposed to electronic access to digital assets.

NRC Response:
The Commission agrees in part. The Commission agrees that not all personnel who require access to SGI also require access to the PA. The Commission disagrees that passwords are not access control devices. The Commission has concluded that the distinction between physical and electronic access is not relevant for this requirement. Specific access controls are applied consistent with the media used.

Comment Summary:
Another commenter stated that the proposed 10 CFR 73.55(g)(6)(ii)(A), in combination with the proposed 10 CFR 73.55(g)(6)(ii) would require SGI combinations/locks to be distributed to only those with unescorted access. The commenter stated that this is a new requirement that is not based in the current rule or NRC Order requirements. Thus, the commenter recommended that the Commission reword the provision such that SGI container access control devices are excluded from this requirement (e.g.,delete "unescorted" from the provision).

NRC Response:
The Commission agrees that not all personnel who require access to SGI, also require access to the PA and has revised the final rule in 10 CFR 73.55(g)(6)(i) to delete the term safeguards information.

Comment Summary:
One commenter stated that the Commission should delete the phrase "to include name and affiliation" from 10 CFR 73.55(g)(6)(i)(B) to make the language performance-based. Also, the commenter stated that maintaining a list of passwords is contrary to basic password protection paradigm that only the individual has access to his password. The commenter recommended

that the NRC replace the phrase “and implement a process to account for access control devices at least annually” with “and implement a process to account for physical access control devices at least annually.”

NRC Response:
The Commission disagrees. The Commission has determined that access devices must be protected, controlled, and accounted for. To accomplish this, a record containing basic information that identifies the individual to whom the device is issued must be established and maintained. The Commission disagrees that this provision requires a list of passwords. This provision requires only that the name and affiliation of the individual to whom a password is issued be recorded and that a methodology to ensure that passwords have not been compromised and are deleted when no longer needed is implemented. The Commission has concluded that this requirement is a fundamental foundation for all access device control programs and therefore appropriately updates the regulatory framework to address this new technology consistent with existing physical protection program requirements.

Comment Summary:
Two commenters stated that 10 CFR 73.55(g)(6)(ii)(C), (D), and (E) do not apply to passwords. One commenter stated that industry-accepted information technology (IT) security practices address the disabling of privilege user access on critical devices. The other commenter stated that the proposed 10 CFR 73.55(g)(6)(ii)(C), (D), and (E) imply that an integrated directory management system may be necessary to reliably disable compromised accounts in a timely manner. The commenter argued that this type of account management system is not common for most process control vendors and several years may be necessary for vendors to incorporate this functionality into their systems. Thus, the commenter recommended that the Commission delete “passwords” from these provisions.

NRC Response:
The Commission disagrees. The Commission has concluded that both commentors have implied meaning that is not supported by the written rule text. The Commission’s expectation is that the licensee will know to “whom” passwords are issued, will know “why” that individual requires access, will know to what protected systems that person has access, and will have in place a capability to discontinue that access when no longer needed. The Commission has concluded that when any access control device is compromised, actions must be taken to prevent that device from being exploited.

The Commission agrees that this requirement is intended to be consistent with current industry-accepted IT security practices that address the disabling of privilege user access on critical devices. This is a fundamental security concept to all security programs regardless of what media the device is based on. The Commission disagrees with the comment regarding an integrated directory management system. The Commission has determined that this comment is not supported by the proposed rule as written.

Comment Summary:
Referencing proposed 10 CFR 73.55(g)(6)(i)(A), one commenter stated that this provision allows identification badges to be removed from the PA when measures exist to confirm the identity of the person returning with the badge. The commenter asked: “Does facial recognition by access control officers suffice?”

NRC Response:

The Commission does not consider facial recognition, alone or absent comparison against a photo ID badge, to be a sufficient methodology to "confirm" the true identity and access authorization of an individual. The Commission requires that at least two unique forms of identification be used and this position has been provided to industry in guidance. Current methodologies include the use of a photo ID badge in conjunction with biometrics.

Comment Summary:
One commenter noted that, in recent years, the Commission has relaxed the requirement to change-out all access control devices when the individual departed voluntarily or was terminated not-for-cause. The commenter stated that proposed 10 CFR 73.55(g)(6)(ii)(E) reinstates the more strict requirement of changing-out all devices regardless of reason for the employee's departure. The commenter asked for clarification of the Commission's intent with respect to this provision.

NRC Response:
This proposed requirement was intended to be a generic requirement to ensure persons who no longer require access are denied access consistent with pre-existing practices and procedures. The Commission has determined that this requirement is sufficiently addressed in the final rule in 10 CFR 73.55(g)(6)(i)(A) which requires that access control devices be issue to only those personnel who require access. When access is no longer needed, that individual no longer meets 10 CFR 73.55(g)(6)(i)(A), and the licensee must follow written procedures that for withdrawing access control devices.

Comment Summary:
A commenter stated that the Commission should modify the provision to "the protected area and vital areas" to clarify that escorted access to vital areas is permitted.

NRC Response:
The Commission agrees. The Commission has revised the final rule to add vital areas.

Comment Summary:
A commenter stated that 10 CFR 73.55(g)(7)(i)(B) should also provide the flexibility for positive identification by personal recognition by an individual with unescorted access who has had sufficient previous contact with the individual to perform this function. Thus, the commenter recommended that the Commission add the following phrase to the end of the provision: "or by an individual with unescorted access who has had sufficient previous contact with the individual to perform this function."

NRC Response:
The Commission disagrees. The Commission has determined that the presentation of identification media is a fundamental and accepted professional standard for initial and recurring visitor processing. The Commission has determined that the suggested relaxation would add no value while decreasing the effectiveness of the visitor control program.

Comment Summary:
See Petition for Rulemaking (PRM) 73-13.

NRC Response:
10 CFR 73.55(g)(7)(i)(F) is added for consistency with 10 CFR 73.56 and NRC response to PRM 73-13. The Commission has determined that where a licensee is aware of derogatory

information that would result in a denial of unescorted access, the licensee shall not then grant escorted access to that individual. The Commission does not intend to require licensees to actively investigate the background of visitors or subject visitors to the requirements of 10 CFR 73.56, but rather, that to comply with this requirement, the licensee must deny escorted access to the individual where the licensee becomes aware of such information through their visitor control procedures or information sharing mechanisms.

Comment Summary:
One commenter stated that 10 CFR 73.55(g)(7)(ii) omits corporate employees who may require frequent but not extended access. Therefore, the commenter argued that corporate employees would not be required to have a photo identification badge, unless "extended access" also implies frequent access over an extended period of employment. The commenter requested that the Commission comment on this issue.

NRC Response:
The Commission agrees in part. The Commission considers corporate personnel to be licensee employees and, therefore, would be processed as an employee for unescorted access where determined necessary by the licensee. This requirement addresses non-employees.

Comment Summary:
Another commenter stated that proposed 10 CFR 73.55(g)(7)(ii) would require photo identification badges to indicate details that do not make sense. The commenter asked several question with regard to this provision: The commenter asked why the badge must indicate "no escort required" when the "non-employee" has been issued a security badge. The commenter noted that industry would already know this information based on the fact that he/she has the security badge. Thus, the commenter concluded that the new requirement does not add value.

NRC Response:
The Commission disagrees that this is a new requirement. This requirement is retained from the pre-existing 10 CFR 73.55(d)(5)(i)(A) and remains valid in support of an effective access control program. This proposed requirement is subsumed in 10 CFR 73.55(g)(7)(ii).

Comment Summary:
The commenter also asked why the badge must indicate "authorized access areas" when access to areas may be changed by an authorized supervisor each month. The commenter argued that the badge itself cannot identify this information, and this information should be stored in the security computer (and associated with the badge number).

NRC Response:
The Commission disagrees that this is a new requirement. This proposed requirement was retained from the pre-existing 73.55(d)(5)(i)(B). However, upon consideration, the Commission concluded that current technology for badging systems have made obsolete the need for such information to be displayed visually on the badge. Therefore, this pre-existing requirement is deleted from the final rule.

Comment Summary:
The commenter asked why the badge must indicate the "period" when the period for which access is authorized may be changed by an authorized supervisor at anytime. The commenter argued that the badge itself cannot identify this information, and this information should be stored in the security computer (and associated with the badge number).

NRC Response:
The NRC disagrees that this is a new requirement. This proposed requirement was retained from the pre-existing 10 CFR 73.55(d)(5)(i)(C). However, upon consideration, the Commission concluded that current technology for badging systems have made obsolete the need for such information to be displayed visually on the badge. Therefore, this pre-existing requirement is deleted from the final rule.

Comment Summary:
The commenter asked why the badge must indicate the employer if the licensee is required to identify "employee" and "non-employee." The commenter noted that this requirement does not add value.

NRC Response:
The Commission agrees. Upon consideration, the Commission concluded that current technology for badging systems have made obsolete the need for such information to be displayed visually on the badge. Therefore, this proposed requirement is deleted from the final rule.

Comment Summary:
The commenter asked why the badge must indicate "assembly area" when an individual's assembly area is subject to change as an individual's work assignment changes. The commenter noted that the badge itself could not identify this information, and this information could be stored in the security computer (and associated with the badge number). Further, the commenter noted that, even if this information is stored, it would be an excessive burden to keep up in the computer. The commenter concluded that this requirement does not add value and signage in the plant is enough. Therefore, this commenter recommended that the Commission delete provisions 10 CFR 73.55(g)(7)(ii) (A) through (E) from the final rule.

NRC Response:
The Commission agrees. Upon consideration, the Commission concluded that current technology for badging systems have made obsolete the need for such information to be displayed visually on the badge. Therefore, this proposed requirement is deleted from the final rule.

Comment Summary:
A third commenter recommended that the NRC delete 10 CFR 73.55(g)(7)(i)(E) from the final rule. The commenter stated that a non-employee who has been granted unescorted access will have completed all training necessary to be granted unescorted access which would have included their emergency assembly area or how to determine the appropriate assembly area.

NRC Response:
The Commission agrees. As stated above, this proposed requirement is deleted from the final rule.

Comment Summary:
Two commenters stated that 10 CFR 73.55(g)(8) implies that all escorts would have to be security personnel, which is not required by the current regulations or Orders. Both commenters concluded that escort training is provided in general employee training and that tracking this training through Appendix B records is not appropriate. Therefore, the commenters recommended that the NRC delete the "appendix B to this part, the approved training and

qualification plan, and" from the provision in the final rule.

NRC Response:
The Commission agrees. The NRC has revised 10 CFR 73.55(g)(8) to delete these references. The Commission's expectation is that facility personnel who are assigned to perform security program duties, will be trained to perform those duties. The Commission does not require that such personnel be trained as a member of the security force, but rather that they are trained to perform the specific duties assigned to them. The Commission agrees that the intent of this requirement could be satisfied by General Employee Training or other generic site training used by the licensee for non-security facility personnel who are assigned to perform security program related duties.

Comment Summary:
Alternatively, one commenter recommended that the Commission should clarify the SOCs with regard to what portions of Appendix B would be applicable to escorts.

NRC Response:
As stated above, the Commission has revised 10 CFR 73.55(g)(8) to delete the references to Appendix B. The Commission's expectation is that facility personnel who are assigned to perform security program duties, will be trained to perform those duties. The Commission does not require that such personnel be trained as a member of the security force, but rather that they are trained to perform the specific duties assigned to them. The intent of this requirement could be satisfied by General Employee Training or other generic site training used by the licensee for non-security facility personnel who are assigned to perform security program related duties.

Comment Summary:
Another commenter stated that the proposed rule allows escorts to take multiple visitors with minimal background checks into protected and VAs within nuclear power plants, but does not require that the escorts meet even minimal physical and visual capabilities. The commenter stated that, unlike the proposed new requirement the Commission seeks to add that unarmed members of the security organization meet specified physical capabilities, the proposed regulations in 10 CFR 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.

NRC Response:
The Commission disagrees. The NRC requires that non-security/facility personnel performing security duties must possess the knowledge, skills, and abilities to effectively perform those duties. Therefore, where assigned duties require sight and hearing capabilities, then the escort is required to possess sight and hearing capabilities to the degree needed to perform those duties. The Commission has revised 10 CFR 73.55(d)(3) to clarify the training and qualification standards for non-security personnel implementing any part of the physical protection program.

Comment Summary:
A commenter stated that the proposed 10 CFR 73.55(g)(8)(i) would require escorts to have unescorted access to all areas in which they will perform escort duties. The commenter argued that this is unnecessary because to gain access to the PA or any VA, an individual first must have been given access to those areas as required elsewhere in proposed 10 CFR 73.55 and 10 CFR 73.56 regarding unescorted access (e.g., proposed 10 CFR 73.55(g)(1)(ii), (g)(1)(iii),

and (g)(2)). Therefore, the commenter recommended that the Commission delete this provision from the final rule.

NRC Response:
The Commission disagrees with the suggestion to delete this requirement. The Commission agrees that access authorization requirements apply to escorts consistent with this final rule. The escort must otherwise already have been authorized and granted access to the area(s) within which the individual will be performing escort duties.

Comment Summary:
One commenter noted that 10 CFR 73.55(g)(8)(ii) is a new requirement that is not required by the Security Orders. The commenter argued that current communications capabilities at the facilities are sufficient for escorts to make notifications or requests for assistance; therefore, the Commission should delete this provision from the final rule.

NRC Response:
The NRC disagrees that this is a new requirement and has determined that this requirement is a fundamental capability for all escorts and is an appropriate update to Commission regulations. The Commission agrees that all licensees should already be in compliance with this requirement and this requirement is consistent with these current licensee practices for providing communication capabilities to an escort. The term "timely" refers to the ability to call for help and complete a response to prevent radiological sabotage. The Commission has revised the final rule to provide flexibility to licensee who choose not to use the CAS/SAS to initiate a response, provided the capability to interdict and neutralize the threat is maintained.

Comment Summary:
Another commenter noted that the proposed 10 CFR 73.55(g)(8)(ii) would require any escort, including non-security escorts, to carry a security-radio and be specifically trained on its operations and how to properly communicate with CAS/SAS. The commenter stated that this implies that a potential threat exists which is not based on historical experience. Since visitors are required to be processed just like anyone else who enters the PA, no prohibited items would be in the visitor's possession. Therefore, no threat would exist to the facility from an authorized visitor under the escort of an authorized site worker with unescorted access. Hence, the commenter recommended that the Commission delete this provision from the final rule.

NRC Response:
The Commission disagrees that this requirement is invalidated simply because it has never happened, and with the assumption that a visitor can not become a threat simply because the visitor was processed through access control equipment. The Commission has determined that timely communication is necessary to ensure that the escort can summon assistance when needed and that this requirement is a fundamental physical protection program element critical to an effective physical protection program.

Comment Summary:
One commenter stated that continuous communication is a new requirement that is not required by the Security Orders. Therefore, the commenter recommended that the Commission delete "continuous" from this provision in the final rule.

NRC Response:
The NRC disagrees that this is a new requirement and has determined that this requirement is an appropriate update to the regulatory framework. The current 10 CFR 73.55(f)(1) requires security personnel to maintain continuous communication capability with CAS/SAS. The current 10 CFR 73.55(d)(4) requires vehicles, to be escorted by security personnel while inside the PA. The amended 10 CFR 73.55(g)(5)(ii) relieves the licensee from the current 10 CFR 73.55(d)(4) and allows facility personnel to escort vehicles inside the PA. In providing this relief, the Commission has determined that it is prudent to "retain" the current requirement for continuous communication capability that was present through the use of security personnel escorting vehicles. Therefore, the Commission retains this current requirement for facility personnel escorting vehicles inside the PA. This requirement does not apply to vehicles operated by authorized facility personnel.

Comment Summary:
Another commenter stated that the proposed 10 CFR 73.55(g)(5)(ii) would allow vehicle escorts by non-security escorts. Therefore, the proposed 10 CFR 73.55(g)(8)(iii) would require any vehicle escort, including non-security escorts, to carry a security-radio and be specifically trained on its operations and how to properly communicate with CAS/SAS. The commenter argued that that this provision implies that a potential threat exits which is not based on historical experience.

The commenter also noted that, as required by the proposed 10 CFR 73.55(g)(5)(iv), vehicles carrying hazardous materials must be escorted by an armed security officer who would have radio contact with CAS/SAS. Therefore, no threat would exist to the facility from an authorized vehicle under the escort of an authorized site worker or armed security officer with unescorted access. Hence, the commenter recommended that the Commission delete this provision from the final rule.

NRC Response:
As stated above, the Commission disagrees with the suggestion to delete this requirement. The Commission disagrees that this requirement is invalidated simply because it has never happened. The Commission agrees that this provision requires non-security personnel performing vehicle escort duties, to posses a capability for continuous communication and to be trained on its operations. However, the NRC has revised the final rule to provide flexibility to licensee who choose not to use the CAS/SAS to initiate a response, provided the capability interdict and neutralize the threat is maintained.

Comment Summary:
One commenter stated that 10 CFR 73.55(g)(8)(iv) is a new requirement that is not required by the Security Orders. The commenter stated that the phrase "knowledgeable of those activities that are authorized to be performed within the areas" is broad and impracticable for any one escort to satisfy due to the many different operational, testing, and maintenance activities and various equipment throughout the plant.

The commenter argued that escorts should only be responsible for observing obvious indications of inappropriate behavior. Therefore, the commenter recommended that the Commission delete the phrase "within the areas for which they are assigned to perform escort duties and must also be knowledgeable of those activities that are authorized to be performed" from this provision in the final rule.

NRC Response:
The Commission disagrees that this is a new requirement and that this requirement is impractical. The Commission agrees that there are many different activities and equipment throughout a site and, therefore, it is appropriate for the individual assigned to perform escort duties to be knowledgeable of the activities and equipment for the area(s) in which that person will perform escort duties.

The Commission does not require the escort to be knowledgeable of everything, but rather that the individual have sufficient general knowledge to be able to identify and respond to actions that could pose a threat to the public health and safety. The Commission has revised the final rule to clarify that the level of knowledge required of an escort is general and need not be technically detailed but must be sufficient to recognize unauthorized activities and tampering by visitors.

Comment Summary:
Another commenter noted that the proposed 10 CFR 73.55(g)(8)(iv) would require all escorts (security and non-security) to be knowledgeable of those activities being performed by visitors. The commenter explained that, typically, visitors are brought in to perform special tasks for which they have the required knowledge not available by others on site. The escort will understand their escort duties and generally be knowledgeable of what the visitor is here to do, but will not be knowledgeable of the activity details. Therefore, the commenter argued that it would be impossible to fully comply with the proposed rule and still maintain plant operations in a manner required to protect the health and safety of the public. The commenter recommended that the Commission revise this provision by inserting “escort” before “activities” and deleting the phrase “and must also be knowledgeable of those activities that are authorized to be performed by any individual for which the escort is assigned responsibility”.

NRC Response:
The Commission disagrees. As stated above, the Commission does not require the escort to be knowledgeable of everything, but rather that the individual have sufficient general knowledge to be able to identify and respond to actions that could pose a threat to the public health and safety. The Commission has revised the final rule to clarify that the level of knowledge required of an escort is general and need not be technically detailed but must be sufficient to recognize unauthorized activities and tampering by visitors.

Comment Summary:
One commenter stated that making reference to other requirements in 10 CFR 73.55(g)(8)(v) is redundant. Therefore, the commenter recommended that the NRC delete the phrase, “provided that the necessary observation and control requirements of this section can be maintained by the assigned escort over all visitor activities,” from this provision in the final rule.

NRC Response:
The Commission agrees that the phrase, "of this section," is redundant but reference to observation and control requirements is necessary and retained. The Commission has deleted the stated deterministic ratios to allow licensees to account for site-specific conditions on a case-by-case basis provided proper observation and controls are maintained.

Comment Summary:
Another commenter stated that 10 CFR 73.55(g)(8)(v) would allow a single escort to take more

visitors with minimal background checks into PAs of nuclear power plants than was specified as an external assault force in the recent DBT rulemaking and would allow literally hundreds of visitors with minimal background checks to be escorted into VAs. The commenter noted several problems with this paragraph.

NRC Response:
The Commission has determined that the access controls presented in this rulemaking provide sufficient assurances that the licensee can maintain the capability to detect, assess, interdict, and neutralize threats that may be presented as a result of granting visitor access to the facility.

Comment Summary:
A commenter stated that the PA/VA distinction contradicts the approach taken to physical protection within this regulation. The commenter noted that the proposed 10 CFR 73.55(f)(1) would require licensees to document how target set equipment and elements were developed. 10 CFR 73.2 was revised to add a definition for target set. The commenter argued that the target set requirements and practices do not ensure that all target set equipment and operator actions are confined to VAs, thus some may reside in the non-vital portions of the PAs. The commenter stated that this regulation must limit the number of visitors that escorts take into areas containing target set equipment when those areas are not within VAs.

NRC Response:
The NRC has determined that the revised final rule text in 10 CFR 73.55(f)(3) and (f)(4) appropriately address target set equipment that may not be in a VA or a PA. Visitor access to locations within the PA that contain such equipment is consistent with NRC requirements for target set equipment. Each licensee is required to identify and protect target set equipment. It is important to note that it is a complete target set that must be protected and not the individual components that make up each target set. Therefore, the individual target set component that is located inside the PA could be lost without resulting in the loss of a complete target set. Furthermore, the comment indicated that proposed rule contained a definition for "target set", but the Commission removed this definition from the final rule, and it will be defined in regulatory guidance.

Comment Summary:
A commenter stated that 10 CFR 73.55(g)(8)(v) limits the number of visitors that an individual escort can take into protected and vital areas of nuclear power plants, but it does not limit the total number of visitors within VAs and PAs. The commenter stated that the regulation must limit the total number of visitors inside VAs and PAs of nuclear plants at any given time.

NRC Response:
The Commission disagrees. The Commission has determined that the performance-criteria to be met by the licensee must ensure that the necessary observation and control requirements of this section can be maintained by the assigned escort over all visitor activities and, therefore, is appropriate.

Comment Summary:
A commenter stated that the recently revised DBT regulation requires licensees to protect their facilities from radiological sabotage by up to X number of external attackers. While the Commission has not publicly stated the magnitude of X, the commenter stated that it is generally understood to be on par with the number of visitors that proposed 10

CFR 73.55(g)(8)(v) would allow an unarmed escort to take into a VA of a nuclear plant and half the number of visitors that 10 CFR 73.55(g)(8)(v) would allow an unarmed escort to take into the PA.

Unless the Force-on-Force (FOF) security exercises have demonstrated that the facility can be protected against attempted sabotage by 10 persons within the PA and 5 persons within the VA, the commenter stated that this regulation undermines the entire physical protection program.

The commenter concluded that the final rule must require armed members of the security organization escort visitors into areas of the plant containing target set equipment, prohibit visitors from entering areas of the plant containing target set equipment, and/or require periodic FOF security exercises that demonstrate the capability to prevent sabotage by 10 persons starting from within the PA and by 5 persons starting from within the VA.

NRC Response:
The Commission disagrees. The Commission has determined that the requirements in 10 CFR 73.55(g)(8)(v) establishes the appropriate performance-criteria relative to this concern. The Commission disagrees that armed personnel must be used to escort visitors in areas where target set equipment may be located. Each licensee is required to identify and protect target set equipment and is required to protect a complete target set, not the individual components that make up each target set. Therefore, a target set component could be lost without resulting in the loss of a complete target set. There are many options that could be taken by a licensee to contain unarmed persons as is suggested by this comment. It is the Commission's expectation that the licensee will be prepared to respond to such actions in a timely and effective manner to ensure high assurance of the public health and safety.

Comment Summary:
If the sabotage threat is such that an escort can take 10 visitors into PAs but only 5 visitors into VAs, the commenter said that the final rule must require measures to protect against an escort for more than 5 visitors from accessing VAs. For example, the escort's access rights could be temporarily changed in the security computer to not permit his or her access badge from opening VA doors. Or, the escort could exchange his or her permanent badge for a temporary badge that only opens doors to PAs of the plant. The commenter stated that these measures would protect against the escort accidentally leading a group of more than 5 visitors into VAs and against the visitors overwhelming their escort and using his or her badge for unauthorized entry into VAs.

NRC Response:
The Commission agrees in part. See the Commission response to previous comment above. Licensees are required to meet the performance-criteria established by these regulations relative to controlling the activities of visitors regardless of the site-specific visitor to escort ratios. How the licensee will control access to VAs by escorts must be described in licensee procedures and is subject to NRC inspection. It is the Commission's expectation that the licensee will be prepared to respond in a timely and effective manner to ensure high assurance of the public health and safety.

Comment Summary:
One commenter stated that the Commission should also take into consideration the inclusion of multiple coordinated teams. The commenter noted that attackers should be presumed to use a full range of weapons such as shaped charges, shoulder-fired rockets, mortars, anti-tank

weapons, and large quantities of explosives. The commenter concluded that the explosives, weapons and equipment need not be limited to hand-carried items as stated in current regulations.

NRC Response:
The Commission determined that this comment is outside the scope of this rulemaking. The NRC requires that each license provide protection against the full capabilities of the DBT adversary characteristics as defined by the Commission in 10 CFR 73.1.

Comment Summary:
Another commenter stated that every fuel oil delivery should be tested on-site before it is pumped into the storage tanks.

NRC Response:
The Commission determined that this comment is outside the scope of this rulemaking and must be addressed in site-specific procedures.

Comment Summary:
One commenter stated that the searches should be conducted at each barrier for those items that must be excluded beyond the barrier in order for its design function to be maintained and as necessary to prevent the introduction of items to an area that could impact effective implementation of the protective strategy. The commenter argued that search for items at any barrier that does not meet those criteria is unnecessary. Thus, the commenter recommended that the Commission revise this provision by replacing “other unauthorized materials and devices” with “other items which could be used for radiological sabotage, as required by the protective strategy.”

NRC Response:
The Commission agrees in part. The Commission agrees that searches at any barrier must be for items consistent with the function of that barrier. Specific search criteria are identified through site-specific analysis and the measures needed must focus on the intended function of each physical barrier. The proposed rule’s use of the term "unauthorized" was intended to capture this position. The Commission has revised the final rule to clarify scope and intent.

Comment Summary:
Another commenter referred to the following phrase in the proposed 10 CFR 73.55: “… in which the unauthorized items could be used to disable personnel, equipment and systems necessary to meet the performance objective and requirements of paragraph (b) of this section.” The commenter stated that this provision would have licensees conduct individual searches with little guidance on a vague premise, open to individual interpretation, on what constitutes an item which could be used to disable personnel, equipment, and systems necessary to meet the performance objective and requirements of the proposed paragraph (b). The commenter recommended that the Commission either dictate requirements by inserting the current rule language, “or other items which could be used for radiological sabotage” or completely remove the proposed phrase.

NRC Response:
The Commission disagrees that this provision would have licensees conduct individual searches with little guidance on a vague premise, open to individual interpretation, on what

constitutes an item that must be searched for. The Commission has provided guidance pertaining to this requirement both before and after September 11, 2001. Therefore, the Commission disagrees with the suggested rule text change.

Comment Summary:
A third commenter stated that the search requirement in the proposed 10 CFR 73.55(h)(1)(i) is designed to prevent the introduction of contraband that could disable personnel, equipment, and systems necessary to accomplish the performance objective and requirements in paragraph (b). The commenter noted that paragraph (b) requires diversity and redundancy. Therefore, the commenter asked: "Is the search requirement intended to protect all components of a redundant set, or ensure that both (or more) are not disabled?

NRC Response:
The Commission has revised the final rule text to clarify the scope of this requirement. The Commission does not intend that defense-in-depth be protected but rather that defense-in-depth be provided to ensure the availability of personnel, equipment, and systems, needed to prevent significant core damage and spent fuel sabotage despite the loss of any one element or component of the physical protection program.

Comment Summary:
One commenter stated that 10 CFR 73.55(h)(1) adds new requirements for searches at OCA control points that are not necessary to meet the functions of the barrier at that location. The commenter stated that OCA configurations vary from facility to facility and a broad statement that requires additional search requirements above those currently in place to comply with the current security Orders is impractical and of no benefit.

The commenter said that this and other areas of the proposed rule text that attempt to address requirements at different barriers or locations in a single paragraph results in difficulty in determining the performance-based requirements at the various locations. Thus, the commenter recommended that the Commission separate the performance requirements for each location (i.e., VA, PA, and OCA).

NRC Response:
The Commission disagrees that this provision adds new requirements or requires measures that are beyond current requirements for any area of the facility. The Commission agrees that OCA configurations vary from facility to facility and, as intended in the proposed rule, the specific searches and criteria to be applied must be site specific. For this reason the proposed rule referenced the approved security plans in which this site-specific information must be described. However, to clarify the scope of this requirement, the Commission has revised the final rule to specify that searches must satisfy the physical protection program design requirements and intended function of the barrier at which they are applied.

Comment Summary:
Another commenter stated that the proposed 10 CFR 73.55(h)(1) could be interpreted as requiring licensees to conduct individual searches at OCA turnstiles and all other OCA control points. The commenter argued that this is a substantial increase in manpower and equipment requirements and exceeds all existing requirements. Thus, the commenter recommended that the Commission remove this requirement for the OCA control points under 10 CFR 73.55(h)(1),

with the exception of vehicle control points. The commenter stated that vehicle control points should only be required to conduct DBT threat searches as required. Thus, the commenter recommended that the NRC delete the phrase “the requirements of this section” from the final rule, which would prevent any misinterpretation that person or prohibitive item searches must also be performed at the OCA control points.

NRC Response:
The Commission disagrees that this provision adds new requirements or requires measures that are beyond current requirements for any area of the facility. The Commission agrees that OCA configurations vary from facility to facility and, as intended in the proposed rule, the specific searches and criteria to be applied must be site specific. For this reason the proposed rule referenced the approved security plans in which this site-specific information must be described. However, to clarify the scope of this requirement, the Commission has revised the final rule to specify that searches must satisfy the physical protection program design requirements and intended function of the barrier at which they are applied.

Comment Summary:
A third commenter stated that searching personnel, vehicles, and packages at the OCA is useless unless a means is established to ensure that, after the search, the individual cannot acquire something that would have been subject to confiscation at the search point. The commenter noted that traveling through the OCA, an area that is currently not required to have a 100 percent denial barrier and intrusion monitoring system, would allow the searched individual to acquire contraband, making the search at the OCA checkpoint useless, but expensive.

NRC Response:
The Commission agrees that licensees are not required to apply a 100 percent denial into the OCA as is required of the PA. This rulemaking clearly requires a licensee to analyze site-specific conditions to determine what materials must be prevented from access into facility areas because they can be used to commit radiological sabotage from those areas. Where a barrier is established it must perform a specific function and designated access portals are established to allow access consistent with that function. Items that do not pose a threat from within the OCA need not be searched for.

Comment Summary:
Another commenter noted that the access control points into restricted areas other than the OCA and PA would not be subject to the requirements of proposed 10 CFR 73.55 (h)(1). The commenter recommended that the NRC replace “...into the owner controlled area and protected area...” with “...into the owner controlled area, the protected area, and other restricted areas...”

NRC Response:
The Commission disagrees. The intent of this requirement is to prevent the access of materials or items that can be used to commit radiological sabotage from that area. Nuclear power plants consist of an owner controlled area, protected area, and vital areas. Therefore, reference to "other" restricted areas is not applicable to power reactors.

Comment Summary:
One commenter stated that the Commission should establish procedures that define a search process with the objective of preventing access of unauthorized personnel or materials beyond the barrier that it was designed to prevent.

NRC Response:
The Commission disagrees. The Commission agrees that all searches, at any barrier, must be consistent with the function to be performed by the barrier at which the search is conducted. However, the Commission disagrees that it is the Commission's responsibility to establish "procedures" that define the search process.

Comment Summary:
Another commenter stated that proposed 10 CFR 73.55(h)(2), (h)(2)(i), and (h)(2)(ii) are too general, and could be misinterpreted as requiring personnel search at the OCA for prohibited items. Thus, the commenter recommended that the Commission revise this provision by adding the phrase “as required in the Commission-approved security plans” to the end of the provision.

NRC Response:
The Commission agrees in part. The Commission has revised the final rule to require that the licensee implement search procedures at OCA access portals. It is the responsibility of the licensee to conduct a site-specific analysis to determine if these searches will apply only to vehicles or must include personnel searches to support the physical protection program.

Comment Summary:
A commenter stated that the Commission should clarify that the 10 CFR 73.55(h)(6) criteria applies to PA entry searches. The commenter concluded that searches at other barriers are conducted in a manner to detect those items that are not permitted beyond the barrier.

NRC Response:
The Commission disagrees. The Commission has concluded that vehicle areas to be searched are applicable to both the OCA and PA vehicle search procedures. The Commission has revised the final rule in 10 CFR 73.55(h)(2)(ii) to generically require that the licensee describe in written procedures, the vehicle areas to be searched and items to be searched for at vehicle access portals.

Comment Summary:
One commenter stated that the proposed 10 CFR 73.55(h) is a new requirement if it is intended to be applied to PA entry searches. Further, if this provision is only applied to the current Order requirements, the commenter recommended that the NRC clarify this in the final rule.

NRC Response:
The Commission disagrees. This requirement was intended to be generic to both PA and OCA vehicle searches. The NRC has revised the final rule in 10 CFR 73.55(h)(2) for OCA searches and in (h)(3) for protected area searches to more prescriptively establish these requirements. It is important to note that PA searches are commonly observed via video surveillance monitored by CAS/SAS and the armed response is provided by the armed responders inside the PA at all times.

Comment Summary:
Another commenter asked if either security officer at the vehicle search point is required to have a weapon. The commenter noted that the provision does not specify this.

NRC Response:

The OCA vehicle checkpoint must have an armed response capability. The Commission has revised the final rule to prescriptively require an armed person at the OCA vehicle checkpoint.

Comment Summary:
Referencing this provision as well as proposed 10 CFR 73.55(h)(1) and 10 CFR 73.55(h)(1)(i), one commenter stated that the rule text appears to require the use of both electronic search equipment and physical searches at every area. The commenter argued that either the electronic search or the physical search is acceptable, and the use of the phrase “or other unauthorized materials and devices” is too broad. The commenter stated that the searches should be for unauthorized materials, which if allowed beyond that barrier, could be utilized to disable personnel, equipment, and systems necessary to prevent an act of radiological sabotage that results in significant core damage. Also, the commenter stated that the ability to detect with electronic means any newly developed technology is unrealistic. The commenter concluded by stating that the words “as needed” do not sufficiently qualify the statement.

NRC Response:
The Commission agrees in part. The Commission does not intend that each and every search must be conducted by both equipment and by personnel, but rather that searches by personnel be used when the equipment search is not adequate or cannot positively identify a given item and when a suspicious item is detected. The Commission agrees that searches must focus on items that present a threat. Specific methodologies to be used are specific to the type of search being conducted.

The NRC agrees in part with the comment that the ability to detect with electronic means any newly developed technology is unrealistic. Consistent with the proposed rule SOCs, the reference to future technological advancements was intended to be generic and focused on "other unauthorized materials and devices". The Commission’s intent was to generically account for future technological advancements that the Commission may attribute to the DBT at a future time. The Commission concluded that use of the phrase "items which could be used to commit radiological sabotage" as used in the final rule 10 CFR 73.55(h)(1) appropriately addresses this intent and has deleted the phrase "or other unauthorized materials and devices" from this requirement of the final rule.

Comment Summary:
A commenter stated that the Commission should clarify that the proposed 10 CFR 73.55(h)(6) applies only to the checkpoint established in the OCA. The commenter concluded that applying this requirement to other vehicle search processes is a new requirement that would exceed the Order requirements.

NRC Response:
The Commission agrees in part. The Commission has revised the final rule to require video equipment at the OCA vehicle search area that is monitored by an individual who can initiate a response if needed. It is important to note that the proposed rule intended to be consistent with the current licensee practice of observing PA searches through video equipment monitored by individuals in the CAS/SAS.

Comment Summary:
A commenter stated that the proposed rule does not close a dangerous loophole in current search requirements for law enforcement personnel and security officers. The commenter

noted that the current rule at 10 CFR 73.55(d)(1) states that, “The licensee shall control all points of personnel and vehicle access into a protected area ....” The licensee shall subject all persons except bona fide Federal, State, and local law enforcement personnel on official duty to these equipment searches upon entry to a protected area. Armed security guards who are on duty and have exited the protected area may reenter the protected area without being searched for firearms.”

The commenter stated that proposed 10 CFR 73.55(g)(1) no longer specifically authorizes these exceptions to the search procedures, but would still allow them, subject to Commission review and approval. 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, as approved by the Commission.

NRC Response:
The Commission disagrees. The proposed rule omitted these pre-existing requirements and generically required them to be addressed by the licensee in security plans. The specific provisions addressed by this comment are retained in the final rule from the pre-existing rule. The Commission has determined that retention of these requirements is appropriate and are consistent with NRC requirements for background checks, psychological assessments, and behavior observation (trustworthiness and reliability). It must be noted that armed security personnel are searched prior to reporting for duty and being issued a firearm. This provision simply allows armed personnel to exit the PA with their assigned weapon, to perform official duties and then re-enter without re-search for a firearm that has been issued to them.

With respect to bona fide Federal, State, and local law enforcement personnel on official duty, they are subject to their own trustworthiness and reliability determinations which are outside the scope of this rulemaking. It is important to note that this flexibility does not relieve the licensee of its responsibility to prevent the introduction of unauthorized items or materials that would otherwise be prevented from access and only applies to those weapons or items that are “issued to designated armed personnel in the performance of “official duties”.

Comment Summary:
One commenter stated that the Commission should add a definition of unauthorized materials in 10 CFR 73.2 to clarify that unauthorized materials are materials that are prohibited from entry for the purposes of protection against radiological sabotage. The commenter stated that this is another example of the need to clarify that the search process at different barriers is intended to search for different materials in accordance with the intent of the barrier.

NRC Response:
The Commission disagrees that "unauthorized materials" requires a definition in 10 CFR 73.2. The Commission has revised the final rule to clarify the types of items that are not authorized access through a given barrier are ones that the licensee has concluded, subject to NRC inspection, can be used to commit radiological sabotage if allowed beyond the barrier.

Comment Summary:
A commenter stated that the NRC should clarify that the proposed 10 CFR 73.55(h)(7) applies to PA entry searches. The commenter concluded that searches at other barriers are conducted in a manner to detect those items that are not permitted beyond the barrier.

NRC Response:
The Commission agrees. The Commission has revised the final rule to address PA searches individually and more prescriptively.

Comment Summary:
One commenter stated that the Commission should retain the current rule language in 10 CFR 73.55(d)(1) and (d)(4). The commenter noted that the current security plans provide for the controls necessary to ensure that emergency response personnel and vehicles are bonafide members and equipment are identified and appropriately allowed access. The commenter argued that to require individual approval of exceptions is unreasonable and unnecessary, and this is a new requirement that exceeds the Order requirements.

NRC Response:
The Commission agrees in part. The Commission disagrees that pre-existing rule text should be used but agrees that current NRC-approved security plans address this requirement. The Commission has revised the final rule to clarify the scope of this requirement, provide necessary flexibility, and ensure consistency with current practices. The Commission agrees that a specific list of exempted items in the security plans is an unnecessary regulatory burden and has revised the final rule to allow a more generic description of the types of items that may be exempted to be included in the security plans, with specific details being addressed in licensee procedures.

Comment Summary:
Another commenter stated that the proposed 10 CFR 73.55(h)(8) would require extensive security plan and procedure changes for language which is already clear in the current rule. The commenter argued that this proposed change puts the licensee liable for dictating rules that may be counter to state and local law enforcement policies and raises issues of constitutionality. The commenter concluded that the current rule language is clear and is identified in station procedures; thus, the Commission should reinsert the current rule language.

NRC Response:
The Commission disagrees that pre-existing rule text should be used but has determined that the current NRC-approved security plans address this requirement. The Commission has revised the final rule to clarify the scope of this requirement, provide necessary flexibility, and ensure consistency with current practices.

Comment Summary:
A third commenter stated that this paragraph notes that exceptions to the search requirements "must be submitted to the Commission for prior review." The commenter asked: "does this apply only to exceptions in the initial plan submitted to the NRC pursuant to the revised 10 CFR 73.55, or to all subsequent changes?" If it is the latter, the commenter asked: "why are search requirements held to a higher standard of Federal regulatory review (i.e., requiring prior approval) than other requirements in 10 CFR 73.55?"

NRC Response:
The Commission has determined that the current NRC-approved security plans address this requirement. The Commission has revised the final rule to clarify the scope of this requirement, provide necessary flexibility, and ensure consistency with current practices.

Comment Summary:
In the proposed 10 CFR 73.55(h)(8)(iii), one commenter stated that the NRC should insert “to the extent practicable” after “receiving area.”

NRC Response:
The Commission agrees. The phrase "to the extent possible" is added.

Comment Summary:
Another commenter stated that the Commission should modify proposed 10 CFR 73.55(h)(8)(iii) to clarify that the material is to be searched to the extent practicable, similar to proposed 10 CFR 73.55(h)(8)(ii). Thus, the commenter recommended that the Commission add the phrase “to the extent practicable” after “searched.”

NRC Response:
The Commission has revised the final rule to clarify the scope of this requirement, provide necessary flexibility, and ensure consistency with current practices.

Comment Summary:
One commenter stated that the Commission should clarify proposed 10 CFR 73.55(h)(8)(i) to state that it only applies to the PA.

NRC Response:
The NRC agrees and has revised the final rule, in 10 CFR 73.55(h)(3)(vii), to specify that this requirement applies only to bulk items that are exempted from protected area search requirements.

Comment Summary:
Another commenter stated that proposed 10 CFR 73.55(h)(8)(i) would require an armed escort for all material exempted from search. However, the commenter argued that this is not appropriate for “all” such materials. The commenter noted that NUREG-0908, “Acceptance Criteria for the Evaluation of Nuclear Power Reactor Security Plans,” provided the acceptable guidance for meeting the existing 10 CFR 73.55(d)(3) search requirements. Licensees have constructed their search processes in accordance with this guidance which only requires security officer escort for Category I and II material. Whereas, Category III material must be positively controlled; e.g., stored in a locked area controlled by a person familiar with the material, and Category IV material must be stored in a locked area and opened under the supervision of persons familiar with their content.

Therefore, the commenter argued that not all material exempted from search is required to be escorted by a security officer. As such, there is no threat evidence that support the proposed new 10 CFR 73.55(h)(8)(i) requirement to have Category I through IV material escorted within the PA by an armed security officer. The commenter recommended that the Commission revise this provision by replacing “...escorted by an armed individual who is trained and equipped to observe offloading and perform search activities at the final destination within the protected area” with “...controlled as described in the Commission-approved security plan for admittance into the protected area.

NRC Response:
The Commission agrees in part. The Commission agrees that the procedural details provided by the commenter regarding Cat I through IV materials are applicable, however, in the case of

bulk materials, an armed escort is required until the absence of contraband can be verified. The NRC disagrees with the recommended rule text change because Commission requirements are described in this final rule, not in the licensee security plan. Licensee security plans describe how the licensee will satisfy Commission requirements.

Comment Summary:
One commenter stated that 10 CFR 73.55(h)(1)(iii) is not specific enough regarding search observation requirements. Thus, the commenter recommended that the Commission revise the provision to state: "...and responsibilities required to satisfy the 10 CFR 73.55(h)(7) vehicle search observation requirements."

NRC Response:
The Commission agrees in part. This proposed requirement is deleted from the final rule because this requirement is adequately addressed in 10 CFR 73, Appendix B and need not be repeated here.

Comment Summary:
Another commenter asked if the qualifications of search personnel are spelled-out somewhere.

NRC Response:
This proposed requirement is deleted from the final rule because this requirement is adequately addressed in 10 CFR 73, Appendix B and need not be repeated here.

Comment Summary:
Regarding proposed 10 CFR 73.55(h)(2)(i), one commenter stated that this provision would restrict entry of "prohibited" items versus "contraband." The commenter noted that both the current and proposed Part 73, Appendix B and Appendix G utilize the term "contraband" when referring to detection training and reportability of such material's entry into a controlled area.

The commenter also noted that contraband is defined as "Any illegal item to include unauthorized weapons, explosives, incendiary devices, and other devices or items that could be used to provide significant assistance in an act of radiological sabotage or personnel injury." The commenter recommended that the NRC revise this provision replacing "a prohibited item" with "contraband."

NRC Response:
This proposed requirement is deleted from the final rule because it is adequately addressed in the final rule in 10 CFR 73.55(h)(1).

Comment Summary:
Regarding proposed 10 CFR 73.55(h)(2)(ii), the same commenter stated that the provision and associated SOCs could be interpreted as not allowing the use of technology, such as the Itemizer, to assist in the search process once the fixed search train equipment alarms. Thus, the commenter recommended that the Commission replace the term "fixed" with "fixed or portable."

NRC Response:
The Commission disagrees. This requirement is deleted from the final rule because this requirement is adequately addressed in 10 CFR 73.55(h)(3)(i).

Comment Summary:
One commenter stated that 10 CFR 73.55(i) seems to be unnecessarily complicated by attempting to address new plant construction and currently operating facilities. The commenter argued that requirements for new plants should be separated or each requirement should be identified with exceptions that apply to currently operating facilities. The commenter noted that the requirements for dual, redundant equipment and capabilities for alarm stations is a new requirement that is more stringent than the Order requirements and would result in a significant impact on currently operating facilities. The commenter argued that the proposed language does not consider the various designs currently in use that provide adequate capabilities to effectively implement the protective strategy. The commenter concluded that these new requirements should be bifurcated from the final rule and addressed in separate rulemaking.

NRC Response:
The Commission agrees in part. The proposed rule attempted to address new reactor construction in the proposed 10 CFR 73.55(a)(5) and (6) and pre-existing reactors in the proposed 10 CFR 73.55(i). To clarify which requirements apply to new reactors and which requirements apply to pre-existing reactors, the Commission generically addresses the new reactor requirements in the final rule in 10 CFR 73.55(a)(6) and specifically requires dual and redundant CAS/SAS for new reactors in the final rule in 10 CFR 73.55(i)(4)(iii). The pre-existing requirement 10 CFR 73.55(e)(1) for protection CAS/SAS against a single act is addressed in the final rule in 10 CFR 73.55(i)(4)(i). The Commission disagrees that requirements for new reactors should be addressed in a separate rulemaking.

Comment Summary:
One commenter stated that the Commission should revise 10 CFR 73.55(i)(1) by replacing “early detection” with “detection and assessment of unauthorized persons and activities at a location or time that facilitates the effective implementation of the protective strategy.” Also, the commenter recommended that the term “all threats” in the SOCs should be bounded by the DBT. Also, the commenter suggested that the Commission avoid the term “time lines” in the SOCs, as it has specific connotations for industry that does not apply in this case. Lastly, the commenter recommended that the Commission replace “beginning at the time of failure” with “beginning at the time of discovery” in the SOC.

NRC Response:
The Commission agrees in part. The Commission has revised the final rule to delete the phrase "early detection." The Commission agrees that the term “all threats” as used in the proposed rule SOCs is bounded by the DBT as stated in 10 CFR 73.1. The Commission agrees that the term “time-lines” as used in the proposed rule SOCs does not have the same meaning as when this term is used in relation to contingency response. However, the Commission disagrees with the suggestion to replace the phrase “beginning at the time of failure” with “beginning at the time of discovery” in the SOCs because the statement is inconsistent with the pre-existing 10 CFR 73.55(e)(2) which requires that an indication of an IDS failure be automatically provided.

Comment Summary:
Another commenter stated that proposed 10 CFR 73.55(i)(1) implies that an early warning system would be required beyond the required PA intrusion detection systems. The commenter said that is unclear as to what the phrase “early detection and assessment” was meant to imply. In addition, the commenter stated that proposed 10 CFR 73.55(i)(1) uses the phrase “at all times, “ which means that anytime a PA IDS segment fails, the licensee is in violation of the rule. Thus, the commenter recommended that the Commission modify the provision to state:

"The licensee shall establish and maintain a protected area intrusion detection and assessment system that provides the capability for detection and assessment of unauthorized persons and activities in accordance with the Commission-approved security plan."

NRC Response:
The Commission agrees in part. The Commission has deleted the phrase "early detection" from the final rule. The Commission disagrees that the phrase "at all times" would not allow for equipment failures as such failure is addressed in other paragraphs of this rule. The NRC disagrees with the suggested rule text because Commission requirements are stated in the regulations, not approved security plans.

Comment Summary:
One commenter stated 10 CFR 73.55(i)(2), while requiring that both CAS and SAS have alarm and video equipment, allows that "at least one" (i.e., not both) must be protected in accordance with (e)(6)(v), (e)(7)(iii), and (i)(8)(ii). The commenter stated that the phrase "at least one" appears to offer some relief from the requirement in proposed 10 CFR 73.55(a)(6) that CAS and SAS be equipped to equivalent standards, and to 10 CFR 73.55(a)(6)(ii) requiring equivalent capabilities of detection. The commenter asked if this paragraph is regulatory relief from those sections.

NRC Response:
The Commission agrees. The requirements in the proposed 10 CFR 73.55(a)(6) apply to future reactors only and do not apply to pre-existing reactors.

Comment Summary:
One commenter stated that the proposed 10 CFR 73.55(i)(10)(ii)(A) applies new requirements not prescribed by either the current rule or NRC Orders. The commenter noted that OCA checkpoint over watch is only required from one alarm station, but the proposed rule would require both alarm stations to remotely monitor the OCA checkpoint. Thus, the commenter recommended that the Commission insert "as required in the Commission-approved security plan" after "alarm stations." The commenter stated that this revision would require the licensee to look at the security plan to understand what CCTV systems are required to be monitored from both alarm stations versus just one.

NRC Response:
This proposed requirement is subsumed in the final rule in 10 CFR 73.55(i)(2). The NRC disagrees that this is a new requirement and has determined that it is an appropriate update to Commission regulations relative to the pre-existing 10 CFR 73.55(e)(1) for CAS/SAS and current licensee practices. This requirement does not pertain to the OCA over watch referenced by the commenter. The Commission disagrees with the proposed rule text change because the NRC requirements are stated in the regulations and not licensee security plans.

Comment Summary:
Another commenter, referring to proposed 10 CFR 73.55(i)(10)(ii)(A) and (ii)(B), stated that displaying video technology concurrently at both alarm stations is not consistent with current practice, which is based on requirements delineated in the February 2002 ICM Order (the Order allows display in several other areas in lieu of the alarm stations).

NRC Response:
The Commission agrees in part. The commenter is referring to specific observation

requirements that may be performed outside the CAS/SAS. This requirement relates to only CAS/SAS functions. The Commission has revised the final rule to be consistent with current licensee practices and to clarify that this requirement focuses on assessment. Therefore, the Commission has deleted reference to observation, monitoring, and surveillance.

Comment Summary:
One commenter recommended that the NRC revise 10 CFR 73.55(i)(10)(ii)(C), replacing "detected activity" with "to protected area alarm annunciation."

NRC Response:
The Commission disagrees. The phrase "detected activity" accurately represents the performance-criteria of this requirement and focuses on the assessment of the cause of the alarm, not on the annunciation itself. An alarm annunciation is not assessed, it is the detected activity/cause of the alarm annunciation that is assessed.

Comment Summary:
Another commenter noted that 10 CFR 73.55(i)(10)(ii)(C) requires video technology capable of making positive recognition of activity. The commenter asked what standards exist for judging the positive recognition and will the Commission be satisfied with the video operator's judgment?

NRC Response:
The Commission agrees that assessment is performed by people and that video technology is a tool, therefore, operator judgment is a component of the assessment process. The Commission has provided guidance in this area and compliance with this requirement is subject to NRC inspection and force-on-force testing.

Comment Summary:
One commenter stated that the proposed 10 CFR 73.55(i)(4)(ii) is a significant, high-impact change that exceeds the requirements of the security Orders. The commenter noted that the exact scope and impact of the requirements cannot be assessed with the current language. Thus, the commenter suggested that the Commission bifurcate this requirement from the final rule, assessed for practicality and benefit, and addressed, if appropriate, in separate rulemaking.

NRC Response:
The Commission agrees in part. The NRC disagrees that this requirement is a significant, high impact change and with the suggestion to bifurcate this requirement from the final rule. However, the Commission agrees that the scope of this requirement must be clarified. The proposed rule unintentionally required that uninterruptible power sources (UPS) for intrusion detection systems (IDS) and assessment equipment be protected as a vital area.

The NRC intended to require only that UPS be required for IDS and assessment equipment at the PA perimeter and not to require that UPS be protected as a vital area. Therefore, the NRC has revised the final rule in 10 CFR 73.55(e)(9)(vi)(A) to retain the pre-existing requirement to protect the secondary power supply for "alarm annunciation equipment" as a vital area and has moved the requirement for UPS for IDS and assessment equipment at the PA perimeter to the final rule in 10 CFR 73.55(i)(3)(vii) as a design feature for the IDS and assessment equipment such that UPS need not be protected as a vital area.

Comment Summary:
Another commenter stated that requiring a UPS for all alarm station functions including assessment is impractical. The commenter stated that high mast lighting could reasonably be interpreted to be required for assessment, and a UPS capable of maintaining the high mast lighting system would be burdensome and is not justified based on the results from FOF inspections performed by the NRC.

NRC Response:
The Commission agrees in part. The NRC agrees that not all IDS equipment and video equipment used by a licensee is required to ensure detection, assessment, and response. It is the Commission's expectation that each licensee will provide UPS for IDS and assessment equipment at the PA perimeter. If the effectiveness of assessment at the PA perimeter or within the protective strategy depends on high mast lighting, then the UPS or other methodology, such as low-light technology would be required for adequate protection between the time of loss of offsite power and when secondary power takes over.

Comment Summary:
One commenter stated that the Commission should replace the terms “significant core damage” and “spent fuel sabotage” with the term “radiological sabotage” because “radiological sabotage” is a defined term in 10 CFR 73.2 and the other terms are not.

NRC Response:
The Commission agrees in part. The NRC agrees that alarm stations do not prevent significant core damage and spent fuel sabotage, and therefore, the Commission has deleted reference to significant core damage and spent fuel sabotage from this final rule requirement.

Comment Summary:
Another commenter stated that the proposed text could be interpreted as requiring identical equipment in both the CAS and SAS, which is not required for defense-in-depth and would exceed the requirements of the security Orders. The commenter argued that this is a significant, high-impact change that exceeds the requirements of the Security Orders, whose exact scope and impact cannot be assessed with the current language. The commenter recommended that the NRC bifurcate this provision from the final rule, assessed for practicality and benefit, and addressed, if appropriate, in a separate rulemaking.

NRC Response:
The Commission disagrees that this requirement would necessitate identical equipment in both the CAS and SAS and disagrees with the suggestion to bifurcate this requirement from the final rule.

Comment Summary:
One commenter noted that the Commission uses the term “equivalent capabilities” in proposed 10 CFR 73.55(a)(6)(ii) and the term “functionally equivalent capabilities” in proposed 10 CFR 73.55 (i)(4). The commenter stated that at the March 9, 2007, public meeting the NRC clarified that the intent is that sites need to be able to carry out the functions as described in their plans form either alarm station and it can use various types of equipment. Further, the commenter noted that the NRC agreed that “functionally equivalent” applies only to the items listed in proposed 10 CFR 73.55(i)(4) and that those capabilities need to be accomplished functionally from either the alarm station.

The commenter stated that the terms “equivalent” and “functionally equivalent” as described in the SOCs appear to conflict with the description provided in proposed 10 CFR 73.55(a)(6)(ii). The commenter argued that “functionally equivalent” should not require that the alarm stations be “equally equipped.” The commenter noted that the ambiguous language appears to require that assessment, monitoring, observation, and surveillance capabilities currently performed locally must be incorporated into the alarm stations. Thus, the commenter recommended that the Commission modify the proposed 10 CFR 73.55(i)(4), at a minimum, by using the term “functionally equivalent.”

NRC Response:
The Commission agrees in part. The requirements of the proposed 10 CFR 73.55(a)(6) would have applied to future reactors only and the proposed 10 CFR 73.55(i)(4) to pre-existing reactors. The Commission agrees that pre-existing CAS/SAS need only perform the same functions required by the NRC to survive a single act, whereas, new reactors must be constructed to CAS standards and equally equipped (i.e., redundant). The Commission does not intend to require identical equipment (make, model, serial#, etc.) to be retrofitted in pre-existing CAS/SAS, but rather that whatever equipment is used in either CAS or SAS must be “capable” of performing the same functions for detection, assessment, and communications, that are required to survive a single act and effectively implement the protective strategy. The Commission has revised the final rule to clarify this scope and has deleted the proposed term "functionally equivalent."

Comment Summary:
Another commenter stated that proposed 10 CFR 73.55(i)(4) would require extensive changes in equipment and the alarm station structures for existing licensee facilities. The commenter noted that in most configurations the primary alarm station also contains, in or nearby, the security computer, which if the primary alarm station is taken out, then redundancy to the other station may be jeopardized. The commenter said that because of the location of the primary alarm station, if it was taken out, the full security protective strategy would have failed and the plant would have more major concerns than redundancy of the alarm stations. Thus, the commenter recommended that the Commission remove the phrase “and the licensee protective strategy in the event that either alarm station is disabled” in the last sentence of proposed 10 CFR 73.55(i)(4).

NRC Response:
The Commission disagrees. This requirement is retained from the pre-existing 10 CFR 73.55(e)(1) for protection of CAS or SAS from a single act and updates that requirement consistent with the survivability of the functions performed in the CAS and SAS to support the site protective strategy.

Comment Summary:
Another commenter stated that proposed 10 CFR 73.55(i)(4)(i) and associated SOCs apply a new expectation for preventing single point failure of security systems that were never designed to such standards. The commenter indicated significant design changes would be required before full compliance could be achieved. The commenter stated that these proposed sections prescriptively require complete duplication of capabilities in the two alarm stations, by separate and redundant detection and assessment systems having no common equipment locations. The commenter argued that such duplication would require extensive backfitting at many facilities despite being unnecessary to ensure an effective protective strategy. Thus, the

commenter recommended that the Commission should revise the provision and SOC to be performance-based rather than prescriptive for robustness of security capabilities.

The commenter suggested the following wording for the proposed 10 CFR 73.55(i)(4)(i): "The licensee shall ensure that a single act cannot remove the capability to respond to an alarm, summon offsite assistance, implement the protective strategy, provide command and control, or otherwise prevent significant core damage and spent fuel sabotage."

NRC Response:
The Commission disagrees. The pre-existing 10 CFR 73.55(e)(1) requires that either CAS or SAS survive a single act. The Commission disagrees that these proposed sections prescriptively require complete duplication of capabilities in both alarm stations except for new reactors as stated in the final rule in 10 CFR 73.55(i)(4)(iii). The Commission has determined that this requirement is consistent with the current 10 CFR 73.55(e)(1) and is consistent with the Commission expectations regarding the functions that must be able to be performed by both alarm stations.

Comment Summary:
At the November 29, 2006, pubic meeting, one commenter asked if the term "a single act" is within the confines of the DBT.

NRC Response:
The NRC responded that "a single act" is "absolutely bounded by the DBT." The NRC explained that an important piece of that is the concept of "functionally equivalent." The concept is that no single act would likely takeout the ability to implement the plan by removing both of the security systems.

Comment Summary:
One commenter stated that the Commission should clarify in the SOCs that CAS and SAS operators will not be responsible for monitoring cyber intrusion detection systems for computer networks that are not physical protection detection and assessment systems.

NRC Response:
The Commission disagrees. It is a licensee choice as to whom to assign such duties and responsibilities.

Comment Summary:
Another commenter stated that the proposed 10 CFR 73.55(i)(8)(v) appears to be unusually prescriptive for a performance-based regulation. The commenter requested that the Commission comment on this issue.

NRC Response:
The Commission disagrees that this requirement is overly prescriptive. The Commission has determined that this requirement is necessary to address lessons learned from implementation of current NRC requirements and establishes performance-criteria relative to alarm station operator actions and the ability of both CAS and SAS to perform required functions.

Comment Summary:
A third commenter stated that proposed 10 CFR 73.55(i)(8)(v) implies that implementing procedures will ensure that alarm station operators have the required knowledge. The

commenter stated that this is not possible. The commenter noted that, as indicated in proposed 10 CFR 73.55 (c)(6)(i), implementing procedures simply describe the duties and responsibilities of the alarm station operators. Thus, the commenter suggested that the Commission delete the term “implementing procedures” from this provision in the final rule. Also, the commenter stated that the Commission should clarify that this provision applies to alarms for physical intrusion detection only and does not include cyber intrusion detection.

NRC Response:
The Commission disagrees that this provision should not include cyber security. It is a licensee choice as to whom to assign such duties and responsibilities. The Commission disagrees that implementing procedures cannot ensure that both operators gain the required knowledge. The Commission has determined that it is through the performance of the actions described in implementing procedures that alarm station operators acquire this knowledge.

Comment Summary:
Another commenter stated that the proposed 10 CFR 73.55(a)(6)(i) requires that the CAS and the SAS comply with 10 CFR 73.55(e)(7)(iii), which specifically references the CAS but is silent on the SAS. The commenter asked how this requirement can hold for the SAS if the paragraph included by reference specifically omits the SAS.

NRC Response:
This requirement is applicable to only new reactors and is intended to require that both the central and secondary alarm stations be entirely redundant. The Commission does not intend to apply this requirement at pre-existing reactors unless, that licensee chooses to construct a new reactor inside the existing protected area. In such cases, the new reactor requirements apply.

Comment Summary:
Another commenter stated that proposed 10 CFR 73.55(a)(6)(ii) appears to be misplaced and would be more appropriate for section (i).

NRC Response:
The Commission agrees. The Commission has revised the final rule to move this requirement to 73.55(i)(4)(iii).

Comment Summary:
A commenter stated that the requirement for the equipment to remain operational under all conditions other than “abnormal or severe weather” is not an achievable objective. The commenter stated that conditions that may be considered “normal” for various seasons at a facility may impact on any known technology. Compensatory measures are initiated until the condition is corrected.”

NRC Response:
The Commission disagrees. The Commission has revised the final rule to delete this requirement because it is redundant to the final rule in 10 CFR 73.55(n)(1)(i). The NRC disagrees that this requirement is not an achievable objective. Pre-existing requirements state that each licensee is responsible to maintain physical security equipment in operable condition. The Commission's expectation is that each licensee will account for the effects that site-specific conditions will have on equipment and, thereby, choose equipment that is appropriate for those

conditions.

Comment Summary:
One commenter recommended that the Commission revise the provision to replace “provides early detection and assessment of unauthorized activities” with “effectively implements the site protective strategy.”

NRC Response:
The Commission agrees. The Commission has revised the final rule to delete the term "early detection" and to clarify that these capabilities focus on the design requirements of 10 CFR 73.55(b), to identify indications of tampering or otherwise implement the site protective strategy.

Comment Summary:
Another commenter stated that proposed 10 CFR 73.55(i)(9)(i) and (ii) imply that each licensee must have some form of early warning systems. Thus, the commenter recommended that the NRC remove the word “early” in both 10 CFR 73.55(i)(9)(i) and (ii).

NRC Response:
The Commission agrees in part. The Commission has revised the final rule to delete the term "early detection" and to clarify that these capabilities focus on the design requirements of 10 CFR 73.55(b), to identify indications of tampering or otherwise implement the site protective strategy.

Comment Summary:
One commenter noted that in the approved security plan template (NEI 03-12), the concept of “continual” surveillance does not apply to the VA or PA and surveillance of these areas is on a frequency of “once per shift.” Absent further explanation, the commenter stated that it is difficult to understand the basis for this requirement. The commenter stated that if it is the Commission’s intent to have the same surveillance and monitoring for the OCA, PA, and VA then a basis is needed. Otherwise, the commenter recommended that the Commission delineate the requirements of each of the three areas in the final rule. Further, the commenter stated that surveillance and monitoring programs are designed to ensure that the site protective strategy is effectively implemented, not necessarily for the detection of unauthorized activities. Lastly, the commenter asked for the basis for the requirement to “ensure the integrity of physical barriers or other components?”

NRC Response:
The Commission agrees in part. The NRC has revised the final rule to specify continuous surveillance, observation, and monitoring requirements for the OCA. The Commission agrees that surveillance and monitoring programs serve multiple purposes and has revised the final rule to delete reference to the detection of unauthorized activities. The regulatory basis for the requirement to “ensure the integrity of physical barriers or other components is found in the pre-existing rule in 10 CFR 73.55(g)(1) and in the final rule in 10 CFR 73.55(n)(1), which require the licensee to maintain all security related equipment, to include physical barriers, in an operable condition to ensure that the function required of the equipment or barrier can be performed, for which the term "integrity" is used.

Comment Summary:

Another commenter noted that the proposed 10 CFR 73.55(i)(9)(ii) requires continual surveillance, observation, and monitoring "of all areas identified in the approved security plans as requiring surveillance, observation, and monitoring." The commenter asked: What if the licensee doesn't identify any such areas?" The commenter stated that there does not appear to be a requirement to do so.

NRC Response:
The Commission has revised the final rule to specify applicability to only the OCA. The proposed rule attempted to address this requirement such that affected areas must be identified through site-specific analysis. Areas identified or not identified by the licensee through site-specific analysis are subject to inspection and force-on-force testing.

Comment Summary:
One commenter noted that the NRC Orders did not include a requirement to monitor or conduct surveillance of unattended openings. The commenter argued that 10 CFR 73.55(i)(9)(iv) is redundant with the proposed 10 CFR 73.55(e)(6)(i), (e)(10), and (e)(8)(vi), which discuss surveillance of different barriers. Therefore, the commenter recommended that the Commission delete this requirement form the final rule.

NRC Response:
The Commission agrees in part. The requirement in 10 CFR 73.55(e)(10) focuses on the opening itself, whereas this requirement focuses on the requirement to monitor such openings. Therefore, the Commission disagrees with the suggestion to delete this requirement.

Comment Summary:
Another commenter stated that proposed 10 CFR 73.55(i)(9)(iv) would imply that openings in the OCA barriers, since no OCA IDS is required, must be monitored at some undefined frequency to prevent exploitation. This is not a realistic requirement. If such a provision is needed, the commenter argued that it should focus on the security barriers of significance, which are PA barriers not covered by the IDS (e.g., a seawall where IDS technology is not appropriate due to ocean-spray conditions). Thus, the commenter recommended that the Commission insert "PA barrier" after "Unattended" in the beginning of the provision.

NRC Response:
The Commission disagrees. The Commission's expectation is that each licensee will ensure that any opening, in any barrier, will be monitored to ensure the opening can not be exploited because exploitation would mean that the barrier did not perform its intended function. The Commission has revised final rule text to clarify that the potential for "exploitation" is determined relative to the function being performed by the barrier. Because a VBS is not intended to function as a personnel barrier, the fact that a person could walk through the opening would not be an exploitation of that opening.

Comment Summary:
A third commenter stated that the proposed 10 CFR 73.55(i)(9)(iv) discusses unmonitored and unattended openings, but does not impose the 96 in^2 standard. The commenter asked if the provision should impose the 96 in^2 standard.

NRC Response:
The 96 square inch measurement is used because it is professionally accepted that an opening meeting this dimension is large enough for an average size person to fit through, and thereby,

could exploit or defeat the function of a personnel barrier. The Commission intends this requirement to be generic and performance-based for all barriers not just personnel barriers and therefore, the Commission has deleted the 96 square inches dimension.

Comment Summary:
Another commenter stated that proposed 10 CFR 73.55(i)(9)(iii)(A) implies that only armed security officers can perform required patrols, so there is no basis for this new requirement. Thus, the commenter recommended that the NRC reword the proposed 10 CFR 73.55(i)(9)(iii)(A) to state: "Security patrols shall periodically check designated areas and shall inspect vital area entrances, portals, and external barriers in accordance with the Commission-approved security plans."

NRC Response:
The Commission disagrees. The Commission's expectation is that only armed patrols will be used to satisfy this requirement and that this requirement is necessary to maintain adequate protection. The Commission agrees that the designated areas and the periodicity of checks, which are site-specific, must be described in the NRC-approved security plans. However, the Commission disagrees with the suggested rule text change.

Comment Summary:
The same commenter stated that proposed 10 CFR 73.55(i)(9)(iii)(B) and (C) are not consistent with the DBT guidance provided in the Roy P. Zimmerman letter to NEI, dated April 5, 2004. The commenter noted that that letter stated, "Security personnel shall be trained to recognize and respond to obvious indications of tampering." Thus, the commenter recommended that the Commission revise the proposed 10 CFR 73.55(i)(9)(iii)(B) to state: "Physical barriers must be inspected at random intervals to identify obvious indications of tampering." Accordingly, the commenter recommended that the Commission revise proposed 10 CFR 73.55(i)(9)(iii)(C) to state: "Security personnel shall be trained to recognize obvious indications of tampering as necessary to perform assigned duties and responsibilities as described in the Commission-approved security plan".

NRC Response:
The Commission agrees in part. The Commission disagrees that, as written, this requirement is not consistent with NRC guidance. Guidance describes one acceptable way of satisfying NRC requirements. This requirement is consistent with the pre-existing 10 CFR 73.55(g)(1) which states, "All alarms, communication equipment, physical barriers, and other security related devices or equipment shall be maintained in operable condition." The Commission has revised the final rule to clarify armed patrols. Furthermore, the Commission has added the term "obvious indications of tampering" to the final rule 73.55(i)(5)(vii) to avoid redundancy.

Comment Summary:
Referring to proposed 10 CFR 73.55(i)(9)(iii)(B), one commenter asked who determines the metrics for randomness here, including the length of the interval overall and whether the random interval is on a per shift, per day, or per week basis.

NRC Response:
The Commission addresses "randomness" in guidance, but specific intervals are determined by each licensee through site-specific analysis and is subject to NRC inspection and must satisfy the design requirements in 10 CFR 73.55(b).

Comment Summary:
One commenter asked if proposed 10 CFR 73.55(i)(9)(iii) requires patrols of all redundant sets of equipment.

NRC Response:
Target set equipment is defined. Whether such equipment is redundant or not is irrelevant for the purpose of this requirement.

Comment Summary:
Referring to proposed 10 CFR 73.55(i)(9)(iii)(C), one commenter recommended that the NRC add the word "obvious" after the word "recognize" for consistency with the April 2004 DBT Order (Physical Protection Measures) and the approved security plans.

NRC Response:
The Commission agrees. This change was incorporated into the final rule.

Comment Summary:
A commenter recommended that the Commission change "and" to "or" so that 10 CFR 73.55(i)(9)(v) reads as, "…licensee protective strategy, or implementing procedures."

NRC Response:
The Commission disagrees. The Commission has revised the final rule to delete reference to the licensee protective strategy because these actions are captured by procedures. The Commission has determined that the term "and" is appropriate.

Comment Summary:
One commenter stated that proposed 10 CFR 73.55(i)(10)(i) is vague and should clarify that the video requirements are described in the PSP. Thus, the commenter recommended that the NRC replace "of this section" with "as described in the Commission-approved security plan."

NRC Response:
The Commission disagrees. All requirements are addressed in the regulations, not the licensee security plans. However, the Commission has deleted this proposed requirement because it is redundant to the final rule in 10 CFR 73.55(n)(1)(i).

Comment Summary:
Another commenter stated that the Commission should modify 10 CFR 73.55(i)(10)(i) to state: "The licensee shall maintain in operable condition all video technology used to satisfy the monitoring, or observation, or surveillance, or assessment requirements of this section and available when needed."

NRC Response:
The NRC agrees staff in part. The NRC has deleted this proposed requirement because it is redundant to the final rule in 10 CFR 73.55(n)(1)(i).

Comment Summary:
One commenter recommended that the Commission delete 10 CFR 73.55(i)(10)(iii), because it is not required by the Order. The commenter stated that it is a management issue not a regulatory issue and fatigue requirements are prescribed in the proposed 10 CFR 26.

NRC Response:
The Commission agrees. This requirement is deleted from the final rule. The Commission's expectation is that with the increased use of video technologies throughout the security profession, all licensees will ensure that inattentiveness due to fatigue is addressed by licensee management. This topic is a recognized and documented concern within the security profession.

Comment Summary:
Another commenter asked: "Why does this paragraph impose an alertness standard for video operators but not for other alarm system operators or response personnel? Is there a standard for alertness?"

NRC Response:
Current and retained Commission requirements address the qualification of personnel to effectively perform their assigned duties and responsibilities. This proposed requirement was intended to address a specific concern that is associated only with the use of video technology.

Comment Summary:
A commenter noted that the proposed 10 CFR 73.55(i)(11)(i) is a new requirement and the Order does not include a requirement to illuminate the OCA. The commenter asked for clarification on this section in the March 9, 2007, public meeting. Specifically, the commenter questioned whether the intent was to increase the amount of illumination in the OCA. The commenter noted that the NRC responded that whatever is in the protective strategy is acceptable.

NRC Response:
The Commission agrees in part. The NRC disagrees that this is a new requirement. The NRC has determined that lighting in the OCA is consistent with pre-existing licensee practices. Sufficient lighting is determined through site-specific analysis and must be part of the physical protection program design. The final rule provides flexibility to licensees to use of low-light technology in lieu of lighting in the PA or OCA.

Comment Summary:
Another commenter stated that the proposed 10 CFR 73.55(i)(11)(ii) retains the old deterministic requirement. The commenter noted that the NRC approved NEI 03-012, Section 10.1 and all power reactor licensee security plans with more appropriate performance-based requirements.

NRC Response:
The Commission agrees in part. The Commission did not eliminate the pre-existing 0.2 footcandle requirement but rather approved the use of low-light technology as an option for licensees to choose to use. This requirement ensures that one or the other option is met and establishes the regulatory framework for NRC approval of low-light technology.

Comment Summary:
One commenter stated that proposed 10 CFR 73.55(i)(11)(ii) reinserts quantitative lighting levels which had been removed from all licensee's PSPs. The commenter stated that the Commission should word proposed 10 CFR 73.55(i)(11)(ii) to be consistent with the existing Commission-approved PSP. The commenter noted that, as currently worded, licensees would again have to place temporary lighting underneath temporary structures (e.g., trailers and all

exterior areas that are not accessible). Thus, the commenter suggested that the Commission revise proposed 10 CFR 73.55(i)(11)(ii) to state:

> "Isolation zones and all exterior areas within the protected area shall be provided with illumination sufficient to 1) permit observation or detection of abnormal presence or activity of persons or vehicles within the isolation zone, a protected area, or a vital area; and 2) enable detection of intrusion or penetration or attempted intrusion or penetration of the isolation zone, a protected area, or a vital area, in a manner that assures initiation of an adequate response by the security organization consistent with the Commission-approved security plan performance objectives. The licensee may augment the facility illumination system, to include patrols, responders, and video technology with low-light technology capable of meeting the detection, assessment, surveillance, observation, monitoring, and response requirements as described in the Commission-approved security plan."

NRC Response:
The Commission disagrees. The NRC agrees that this requirement clearly and explicitly retains the pre-existing 0.2 footcandle requirement. The relief granted by the NRC and referred to by this comment, does not eliminate, nor was it intended to eliminate, the 0.2 footcandle requirement but rather it allows the use of low-light technology in facility areas where the 0.2 footcandle requirement is not or can not be met.

This requirement provides a methodology and regulatory framework for licensees to account for site-specific areas where lighting levels do not meet 0.2 footcandle without having to resort to the use of additional or portable lights such as under trailers. The Commission has determined that this comment is addressed through the phrase "to meet the detection, assessment, surveillance, observation, monitoring, and response requirements of this section". Therefore, the Commission disagrees with the suggested rule text change but has revised final rule text to clarify that low-light technology is not capable of meeting the requirements of this section but rather that it is a tool that can be used to meet the requirements of this section.

Comment Summary:
A commenter stated that 10 CFR 73.55(j)(1) is a new requirement; the Order includes no requirement to maintain continuous communication with offsite resources. The commenter argued that the ability to maintain such communication is beyond the ability of licensees. Thus, the commenter recommended that the Commission delete "resources to ensure effective command and control during both normal and emergency situations" from the provision in the final rule.

NRC Response:
The Commission disagrees. The pre-existing 10 CFR 73.55(f)(1) is retained in the final rule 73.55(j)(3) and requires security personnel to maintain the capability for continuous communication with CAS/SAS who can call for offsite Local Law Enforcement Agency (LLEA) support. This requirement focuses on the "capability" to communicate with both on-site security force and off-site LLEA resources when needed. The NRC has determined that this requirement is consistent with current security plans and other site emergency plans.

Comment Summary:
One commenter noted that 10 CFR 73.55(j)(3) is a new requirement for vehicle escorts, and the Commission should describe the vehicle escort communication requirements in NEI 03-12

Section 9.5.

NRC Response:
The NRC has revised the final rule to focus on continuous communication with on-site members of the security organization. The Commission disagrees that this is a new requirement. The pre-existing 10 CFR 73.55(f)(1) requires security personnel to maintain continuous communication capability with CAS/SAS and the current 10 CFR 73.55(d)(4) requires that security personnel escort vehicles in the PA.

Comment Summary:
Another commenter stated that proposed 10 CFR 73.55(j)(3) requires each vehicle escort to have continuous communication with each alarm station, which should not be a requirement. The commenter stated that the final rule should allow for practical considerations associated with the nature of field communications. Thus, the commenter recommended that the Commission revise the provision in the final rule by deleting "vehicle escort" and "continuous."

NRC Response:
The Commission disagrees. The pre-existing 10 CFR 73.55(f)(1) requires security personnel to maintain continuous communication capability with CAS/SAS and the current 10 CFR 73.55(d)(4) requires that security personnel escort vehicles in the PA.

Comment Summary:
Concerning the proposed 10 CFR 73.55(j)(4), one commenter stated that the Commission should retain the current rule language, which is clear and performance-based.

NRC Response:
The Commission disagrees. The Commission determined that these current requirements are appropriately, retained.

Comment Summary:
Another commenter stated that "conventional telephone service" in the proposed 10 CFR 73.55(j)(4)(i) appears to refer to landlines. However, the commenter argued that the cell phone is now so conventional that it could qualify. The commenter stated that if the Commission intends to refer to landlines, the rule should specify this.

NRC Response:
The Commission agrees in part. The Commission has determined that the term "conventional" is appropriately generic and that the focus of this requirement is represented by the term "service". The Commission does not limit telephone "service" to the specific equipment used to access that "service such as landlines. The Commission's intent is to ensure a commonly used communication capability.

Comment Summary:
One commenter stated that national emergency response drills have identified communications as being a persistent problem and satellite phones provide a solution. The commenter stated that commercial phone lines and cell phones are unreliable and problematic during emergencies; therefore, the Commission should require licensees to have at least three satellite telephones.

NRC Response:

The Commission agrees in part. The Commission agrees that communications are a concern for all responding personnel and agencies and acknowledges that each technology has benefits and vulnerabilities, however the Commission has determined that the requirement for telephone service must remain generic so as to not require updating every time a new technology becomes available and must refer to the telephone "service" that is common between all responding agencies. Therefore, the Commission disagrees that it is necessary to require the suggested specific technology in this rulemaking.

Comment Summary:
Another commenter stated that the proposed 10 CFR 73.55(j)(4)(iii) should not be a requirement for escorts. The commenter stated that licensee communication systems were never designed or required to be as robust as required by this proposed rule. The commenter stated that to do so would require significant modifications and funding, neither of which were justified by the SOCs.

Also, the commenter stated that the Commission should clarify if this provision applies to computer system intrusion attempts, and the Commission should define reasonable response that allows for an initial assessment of the problem. Thus, the commenter recommended that the Commission revise the provision by replacing "escorts, local, State, and Federal law enforcement agencies, and all other personnel necessary to coordinate both onsite and offsite responses" with "and local law enforcement authorities as described in the Commission-approved security plan."

NRC Response:
The Commission agrees in part. The Commission has determined that communication capabilities are a fundamental necessity and are essential to the effectiveness of any licensee program. The Commission disagrees that the this provision would require any modification to existing licensee programs other than the possible exception of implementing procedures to ensure that the currently used communication methodologies are identified and coordinated. The Commission disagrees that computer system intrusion attempts need to be identified in this requirement. The Commission determined that only communication with the control room needs to be identified in this requirement because all other entities listed are addressed elsewhere in this final rule.

Comment Summary:
A commenter noted that 10 CFR 73.55(j)(6) is a new requirement and will be virtually impossible to implement given plants' reinforced concrete construction and trip sensitive equipment.

NRC Response:
The Commission disagrees that this is a new requirement. This requirement is intended to ensure that such areas are identified and accounted for in procedures consistent with the pre-existing 10 CFR 73.55(f)(1). The Commission has revised the final rule to clarify that alternative communication may include an intercom system or could also be satisfied through a procedure that accounts for the time it takes for a patrol to pass-through the affected area and re-establish communication the failure of which would result in a response being initiated to determine the cause. These details are addressed in guidance.

Comment Summary:
A commenter stated that the NRC site security regulations for all nuclear power plants, reactor and high level nuclear waste storage, take into account the relative availability of local police.

NRC Response:
The Commission agrees. The final rule, in 10 CFR 73.55(k)(7) requires licensees to develop and document liaison with Local Law Enforcement to account for availability.

Comment Summary:
Another commenter noted that the proposed rule would require only five security guards per shift, up from three.

NRC Response:
The Commission disagrees. The final rule requires that licensees maintain the minimum number of armed responders needed to effectively implement the protective strategy. The specific number of armed personnel required is site-specific and is verified through force-on-force testing. The final rule in 10 CFR 73.55(k)(ii)(B) establishes the pre-existing 10 CFR 73.55(h)(3) requirement for 10 armed responders and explicitly deletes the pre-existing allowance to have five (5) if approved by the Commission.

The proposed rule attempted to address this minimum number in performance-based language, however, upon review, the Commission determined that it is important to clarify the Commission expectation that, although a license may have more than 10 armed responders, the Commission will no longer approve requests for less than 10 armed responders, available to perform response duties, inside the protected area at all times.

Comment Summary:
One commenter recommended that the Commission delete the phrase “at all times,” to reflect requirements in NEI 03-12 section 4.2 of the SCP. Also, the commenter recommended that the NRC replace the terms “significant core damage” and “spent fuel sabotage” with the term “radiological sabotage” because “radiological sabotage” is a defined term in 10 CFR 73.2 and the other terms are not.

NRC Response:
The Commission disagrees. The Commission has determined that “at all times” is appropriate. The final rule, in 10 CFR 73.55(k)(5), requires licensees to have procedures in place to reconstitute the minimum number of response personnel in the event that an individual responders becomes ill or are injured. The Commission retains the terms significant core damage and spent fuel sabotage in the final rule in 10 CFR 73.55(b)(3).

Comment Summary:
Another commenter stated that proposed 10 CFR 73.55(k)(1)(i) would require licensees to apply new protective resources and strategies towards the independent spent fuel storage installation (ISFSI) protection that are not required by current rules or NRC Orders. The commenter stated that the final rule should reference the security plan requirements. Thus, the commenter recommended that the Commission revise this provision by replacing “personnel” with “armed responders and armed security officers” and adding the phrase “as described in the Commission-approved security plan” to the end of the provision.

NRC Response:
The Commission disagrees. This requirement is a generic description leading to requirements for “armed responders and armed security officers” addressed in later subparagraphs. Addressing ISFSIs is an unsupported comment and is a site-specific condition that is not

addressed by this rulemaking.

Comment Summary:
A commenter recommended that the Commission delete and combine proposed 10 CFR 73.55(k)(1)(ii) and (k)(1)(iii) into following paragraph: "(k)(1)(iii)The licensee shall provide, maintain, and describe in the approved security plans, all firearms and equipment to be possessed by or readily available to, armed personnel to implement the protective strategy and carry out all assigned duties and responsibilities. This description must include the general distribution and assignment of firearms, ammunition, body armor, and other equipment used."

NRC Response:
The Commission agrees in part. The NRC agrees that the requirements of 10 CFR 73.55(k)(1)(ii) and (k)(1)(iii) are related and has deleted this requirement from the final rule in 10 CFR 73.55 because it is redundant to Appendix B and Appendix C to Part 73.

Comment Summary:
One commenter stated that proposed 10 CFR 73.55(k)(1)(iii) would require licensees to describe, in detail, what firearms and equipment licensees utilize, which would take licensees back to the pre-NEI 03-12 (security plan template) days when licensees were forced to make frequent security plan changes as they enhanced their protective strategies as equipment aged and technology changed. The commenter noted that the Commission-endorsed NEI 03-12 just requires documenting the minimum requirements that currently exist in 10 CFR 73.55, Appendix B. Thus, the commenter recommended that the NRC insert "as described in Part 73 Appendix B, Section G that are" after "equipment."

NRC Response:
The Commission disagrees with this comment. However, the Commission has determined that this requirement is redundant to the final rule requirements of Appendix B and Appendix C to Part 73 and, therefore, has deleted this requirement from the final 10 CFR 73.55.

Comment Summary:
Another commenter asked that, in requiring the licensee to describe the distribution of firearms and equipment, is the rule referring to how the firearms and equipment will be distributed to individuals during response, or to how the firearms and equipment are distributed in locked cabinets on a routine basis?

NRC Response:
The Commission has deleted this requirement from the final 10 CFR 73.55 because it is redundant to Appendix B and Appendix C to Part 73.

Comment Summary:
One commenter stated that proposed 10 CFR 73.55(k)(2) only recognizes state law, but some licensee facilities are located on a federal reservation where federal law is also applicable. Thus, the commenter recommended that the Commission add "and/or federal law" to the end of the provision in the final rule.

NRC Response:
The Commission agrees. The final rule is revised to include federal law enforcement agencies that may have jurisdictional authority for some sites.

Comment Summary:
Another commenter stated that the proposed 10 CFR 73.55(k)(2) is a key section of the rule and one that allows the use of deadly force against adversaries. However, the commenter noted that it is based on threats to individuals and not to the safety systems of the plant. The commenter asked: "Under the EPAct of 2005, are security officers permitted to use deadly force against intruders who appear determined to disable or destroy safety systems and/or target sets? If not, does the 'defense of others' phrase refer to others throughout society?"

NRC Response:
State and federal laws govern the use of deadly force depending on which has jurisdictional authority over the site.

Comment Summary:
One commenter stated that for cases where a plant does not have armed security officers, the Commission should revise the final rule to state: "The licensee shall provide an armed response team consisting of armed responders and armed security officers, to carry out response duties as described in approved security plans."

NRC Response:
The Commission agrees in part. The NRC has revised the final rule, in 10 CFR 73.55(k)(4), to clarify that the use of armed security officers is a site specific determination and are not "required" except as identified by the licensee in the protective strategy and stated in NRC-approved security plans.

Comment Summary:
Another commenter stated that the final rule should ensure that security officers with duties other than immediate armed response are not required for protection against the DBT and are not inappropriately credited in FOF exercises. The commenter noted that the proposed rule requires that licensees provide an armed response team consisting of both "armed responders" and "armed security officers." The commenter explained that the difference between the two terms is that "armed responders" cannot be assigned "any other duties or responsibilities that could interfere with response duties." "Armed security officers," on the other hand, can be assigned such duties or responsibilities. Therefore, the commenter argued that the Commission should write the final rule to clarify that only "armed responders" can be utilized in the protective strategy to protect against the DBT.

NRC Response:
The Commission agrees in part. This issue is specifically addressed by this final rule in 10 CFR 73.55(k) which requires that licensees document, in the Commission-approved security plans and site protective strategy, the minimum number of armed responders who are inside the protected area and are available at all times to perform response duties. Armed responders may not be assigned other duties. This requirement also allows the licensee to supplement armed responders with armed security officers, who are onsite and available at all times to perform response duties during contingency events, if the armed security officers are trained, qualified and equipped to perform these response duties and the minimum number of armed security officers is specified in the NRC-approved security plans and site protective strategy.

The Commission agrees that because armed security officers are not required for immediate response, they may be assigned other duties. However, if used, the licensee is required to specify the duties that armed security officers will perform within the protective strategy and is

responsible for ensuring that other assigned duties, not required by the protective strategy, do not prevent the armed security officers from meeting their response duties and timelines as specified by the protective strategy.

For the purposes of force-on-force testing, a licensee may use less than the documented number of armed responders and armed security officers, but is explicitly prohibited from using more than the minimum number stated in the approved security plans and protective strategy. Therefore, the Commission disagrees with the recommendation to limit a licensee to only utilize armed responders designated in the Commission-approved security plans and site protective strategy to protect against the design basis threat and for the purpose of force-on-force testing.

Comment Summary:
One commenter recommended that the Commission include PA access point in the proposed 10 CFR 73.55(k)(3)(i)(B). Thus, the commenter stated that the Commission should insert "or at a PA access point" after "protected area."

NRC Response:
The Commission disagrees. The NRC has determined that armed responders may be located at a PA access portal provided that these personnel remain physically inside the PA and are able to meet response timelines required by the licensee protective strategy.

Comment Summary:
Another commenter agreed that a PA guards' sole responsibility is inside the PA.

NRC Response:
No response necessary.

Comment Summary:
One commenter stated that the proposed 10 CFR 73.55(k)(3)(iv) is redundant with the proposed 10 CFR 73.55(k)(1)(ii). Thus, the commenter recommended that the NRC delete this provision from the final rule.

NRC Response:
The Commission agrees. The NRC has deleted this requirement from the final rule because it is redundant to Appendix B and Appendix C to Part 73 and the final rule in 10 CFR 73.55(n)(1)(i).

Comment Summary:
Two commenters stated that proposed 10 CFR 73.55(k)(3)(iv) is redundant to the proposed 10 CFR 73.55(k)(1)(iv). One commenter stated that the Commission should delete proposed 10 CFR 73.55(k)(3)(iv) from the final rule.

NRC Response:
The Commission agrees. The NRC has deleted this requirement from the final rule because it is redundant to Appendix B and Appendix C to Part 73 and the final rule in 10 CFR 73.55(n)(1)(i).

Comment Summary:
A commenter asked: "In the event of a strike, would work hours limitations be waived?"

NRC Response:
A strike condition must be considered by each licensee and pre-determined plans for strike conditions would be implemented. The Commission requires the licensee to maintain the minimum number of armed response personnel stated in their NRC-approved plans at all times. This requirement focuses on events such as illness or injury and the procedures to be followed to re-establish the minimum number.

Comment Summary:
A commenter asked: "Is the protective strategy subject to NRC review/approval? Is it incorporated by reference into some licensing document?"

NRC Response:
The licensee protective strategy is not subject to Commission review and approval. The protective strategy is similar to an implementing procedure which is subject to frequent change and is tested through force-on-force exercises. Therefore, the Commission has determined that it is not effective, nor efficient to require the protective strategy to be reviewed and approved by the NRC.

Comment Summary:
One commenter noted that 10 CFR 73.55(k)(6) is a new requirement not required by the Order. The commenter argued that only appropriate facility personnel should be required to receive periodic training as to their responsibilities in responding to hostage and duress situations.

NRC Response:
The Commission agrees in part. The Commission has deleted this proposed requirement from the final rule because it is inclusive to licensee training programs. The Commission's expectation is that all employees present in the PA at the time of a security event have basic knowledge of what actions are expected of them to ensure security actions can be carried out without interference from or danger to that employee.

Comment Summary:
Another commenter stated that the proposed 10 CFR 73.55(k)(6) is more stringent than the original NRC ICM Order requirements. In addition, the commenter noted that the phrase "security incidents" is undefined and confusing. Lastly, the commenter argued that this provision is redundant, in some aspects, to proposed 10 CFR 73.55(c)(4)(ii). Thus, the commenter recommended that the Commission replace "all personnel authorized unescorted access to the protected area are trained and understand their roles and responsibilities during security incidents, to include hostage and duress situations" with "appropriate plant personnel maintain an ability to respond to a hostage or duress situation" in this provision of the final rule.

NRC Response:
The Commission disagrees. The Commission has deleted this proposed requirement from the final rule because it is inclusive to licensee training programs. The Commission's expectation is that all employees present in the PA at the time of a security event have basic knowledge of what actions are expected of them to ensure security actions can be carried out without interference from or danger to that employee.

Comment Summary:
One commenter asked if this provision requires training for all personnel on site (including administrative, clerical, janitorial), or if the phrase should be "trained in their roles and

responsibilities relating to response to security incidents."

NRC Response:
The NRC intended that all personnel inside the PA be trained. The Commission has deleted this proposed requirement from the final rule because it is inclusive to licensee training programs. The Commission's expectation is that all employees present in the PA at the time of a security event have basic knowledge of what actions are expected of them to ensure security actions can be carried out without interference from or danger to that employee.

Comment Summary:
A commenter recommended that the Commission merge the proposed 10 CFR 73.55(k)(7)(i) and (ii) to state: "Determine the existence and level of the threat through the use of assessment methodologies or procedures."

NRC Response:
The Commission agrees. The NRC has revised final rule text.

Comment Summary:
A commenter recommended that the NRC delete "intercept" from 10 CFR 73.55(k)(7)(iii) because response strategies do not require interception.

NRC Response:
The Commission agrees in part. The Commission has revised the final rule for consistency with the final rule in 10 CFR 73.55(b)(3)(i). The Commission has revised the final rule to replace the terms "intercept", "challenge", and "delay" with the single term "interdict".

Comment Summary:
A commenter noted that the proposed 10 CFR 73.55(k)(7)(iv) is a new requirement and the Order does not require notification of off-site agencies other than local law enforcement. The commenter recommended that the Commission revise the provision to state: "Notify local law enforcement, in accordance with site procedures."

NRC Response:
The Commission agrees in part. The Commission has revised the final rule to specify LLEA. However, the Commission's expectation is that each licensee will determine the off-site support needed to respond to an event and will follow its own procedures for notifying offsite support agencies.

Comment Summary:
One commenter noted that 10 CFR 73.55(k)(8) is a new requirement and the Order does not require agreements with agencies other than local law enforcement. Thus, the commenter recommended that the Commission retain the language in current 10 CFR 73.55(h)(2).

NRC Response:
The Commission disagrees because this requirement retains the pre-existing 10 CFR 73.55(h)(2). This requirement is not intended to be "all inclusive" (i.e., agreements with all three agencies), however, this requirement is intended to generically account for those sites whose LLEA is a state or federal law enforcement agency.

Comment Summary:

Another commenter stated that proposed 10 CFR 73.55(k)(8) should only refer to the requirements in Part 73 Appendix C. The commenter argued that the phrase "document and maintain current agreements with local, state, and Federal law enforcement agencies" is not appropriate for all licensees. Thus, the commenter recommended that the Commission revise this provision in the proposed rule by replacing "document and maintain current agreements with local, state, and Federal law enforcement agencies, to include estimated response times and capabilities" with "maintain an integrated law enforcement response plan in accordance with Part 73 Appendix C."

NRC Response:
The Commission disagrees because this requirement retains the pre-existing 10 CFR 73.55(h)(2).

Comment Summary:
Multiple comments

NRC Response:
The NRC has revised final rule text in 10 CFR 73.55(l) to include a maximum 20 weight percent of plutonium dioxide (PuO2) in MOX fuel assemblies. Weight percents of greater value will require Commission approval and is discussed in the revised 10 CFR 73.55(l)(7). The Commission has revised final rule text to move the applicability statement and protection against theft and diversion statement of this requirement to 10 CFR 73.55(l)(1).

Comment Summary:
One commenter stated that the requirements in 10 CFR 73.55(l)(1) of the proposed rule are technically unsupportable, irresponsible, and set a dangerous precedent. The commenter believed that this section of the proposed rule should be removed. The commenter provided several arguments in support of this suggestion. First, the commenter explained that this section of the proposed rule substitutes security requirements for unirradiated MOX fuel assemblies. The commenter stated that this substitution is inadequate and will not result in the necessary level of protection. The commenter urged the Commission to revise the SOCs to remove any suggestion that the proposed rule language strengthens security requirements.

NRC Response:
The Commission disagrees. The NRC has determined that the requirements of this paragraph provide the appropriate regulatory framework and minimum security measures necessary for the protection of MOX fuel assemblies at NRC licensed nuclear power reactor facilities. These requirements are necessary for adequate protection of MOX fuel assemblies considering the size, configuration, and form of the nuclear material.

Comment Summary:
The commenter also stated that through this proposed rulemaking, the Commission is ignoring the Atomic Safety and Licensing Board's (ASLB's) decision in the Catawba case. In that case, the ASLB added security conditions to Duke Energy's proposed security plan. One of the ASLB's conditions is not in the proposed rule.

The commenter also argued that the NRC did not define MOX fuel in the proposed rule (with regard to concentration, weight, or any other physical property), and suggests that this is necessary. Finally, the commenter disagreed with the fact that the proposed rule language does not make a distinction between the security applied to a small number of MOX lead test

assemblies (LTAs) and the security applied to a large number of assemblies. Given all of these issues, the commenter urged the Commission to delete this section from the proposed rule.

NRC Response:
The Commission disagrees. The requirements of this 10 CFR 73.55(l)(1) incorporate Commission direction relative to the site-specific security measures applied at Catawba. The Commission considered the further ASLB recommendations and determined that these additional measures were not necessary for adequate protection and directed that the security measures to be implemented should be in alignment with the Commission's initial position.

In addition, the Commission has determined that the security measures addressed by this paragraph apply for the protection of MOX fuel and, therefore, there is no need to distinguish between a small or large number of assemblies. The Commission disagrees that MOX fuel should be defined in this rulemaking and has determined that an adequate characterization of MOX fuel is provided in draft regulatory guidance for MOX fuel.

Comment Summary:
Another commenter volunteered to address any questions and provide subject matter expertise for any comments related to mixed oxide fuels.

NRC Response:
The Commission has determined that this offer of assistance is not appropriate for the rulemaking process.

Comment Summary:
A commenter stated that the rationale the NRC provides for relaxing security for MOX fuel does not justify the proposed generic lowering of security for such material. The commenter explained that a terrorist's ability to extract plutonium from MOX would depend on the terrorist's experience. The commenter further suggested that fuel assemblies are heavy and awkward only if they remain intact. Finally, the commenter stated that the NRC should not rely on predictions about terrorists' intentions, instead of their capabilities, dedication, and objectives.

NRC Response:
The Commission disagrees. The NRC disagrees that the security measures for MOX fuel is relaxed by this rulemaking because plutonium dioxide in this configuration is a new application not addressed in pre-existing regulations. The Commission has determined that due to the low plutonium weight percentage or concentration in the MOX fuel, certain requirements for CAT I materials are unnecessary regulatory burden and, therefore, this paragraph establishes the appropriate regulatory framework for the physical protection of un-irradiated MOX fuel assemblies. The requirements addressed in this section focus on protection against the DBT of radiological sabotage while the requirements of paragraph 10 CFR 73.55(l) provide additional requirements including protection against theft and diversion of MOX fuel assemblies.

Comment Summary:
One commenter stated that the term "search" in 10 CFR 73.55(l)(3)(iii)(B) is not clear. The commenter explained that the Commission does not provide a reason for why MOX assemblies would require a "search" for security reasons when regular fuel does not. The commenter also suggested that the requirement for a tamper indicating device in 10 CFR 73.55(l)(3)(ii) would obviate the need for a search. An intact tamper indicating device at fuel receipt provides high assurance that the fuel is in the same state as when it was shipped. The commenter urged the

Commission to delete this requirement.

NRC Response:
The Commission disagrees that the use of a tamper indicating seal obviates the need for a search. A tamper indicating seal is one level of protection to be used in conjunction with others to provide defense-in-depth. As stated in the final rule, in 10 CFR 73.55(l)(3)(iv), the licensee may choose to conduct both inspection and search of the MOX fuel assembly simultaneously. The Commission has determined that the search of MOX fuel assemblies is necessary and appropriate to assure adequate protection of MOX fuel assemblies and is consistent with other NRC requirements for inspection of MOX fuel assemblies for damage.

Comment Summary:
With regard to 10 CFR 73.55(l)(3)(vi), the commenter stated that a licensee already has a material control and accountability (MC&A) program for the spent fuel pool in which the MOX assemblies are stored. The commenter suggested that a unique program for only the MOX assemblies is unnecessary and would result in a greater potential for errors. The commenter suggested that MOX assemblies be controlled and accounted for under the licensee's existing MC&A program. The commenter urged the Commission to delete this proposed provision.

NRC Response:
The Commission agrees in part. The NRC disagrees with the suggestion to delete this requirement. However, the Commission agrees that the existing licensee MC&A programs may be used to account for MOX fuel assemblies. The Commission has determined that it is prudent and necessary to document and maintain records that positively identify MOX fuel assembly locations within the spent fuel pool.

Comment Summary:
With regard to 10 CFR 73.55(l)(3)(vii), the commenter stated that it is hard to see how this requirement would be implemented without controlling the entire MC&A database as SGI, which, according to the commenter, is impractical. The commenter suggested that handling fuel prior to and during an outage would be especially difficult if all records of MOX assembly locations are controlled as SGI. For lead assemblies, the Commission did not require the locations to be controlled as SGI. The commenter suggested that the proposed requirement is unneeded and should be deleted.

NRC Response:
The Commission agrees. The NRC acknowledges that 10 CFR 73.55(l)(3)(vi) intends that the existing MC&A recordkeeping system may be used and that this provision could necessitate that the entire MC&A database be marked as SGI. The Commission has determined that the protection of MC&A records must be evaluated against the criteria of 10 CFR 73.21 to determine if such information must be protected and that a blanket requirement to protect MOX fuel MC&A records as SGI is an unnecessary regulatory burden. Therefore, the Commission has deleted this proposed requirement from the final rule.

Comment Summary:
One commenter suggested that the NRC rewrite 10 CFR 73.55(n)(1) to require licensees to review the security program 12 months following initial implementation and then at least every 24 months, or as currently approved in the security plan.

NRC Response:
The Commission agrees. The NRC has revised 10 CFR 73.55(m)(1) by addressing the overall 24 month requirement first and addressing the conditional 12 month periodicity in the final rule in 10 CFR 73.55(m)(1)(i).

Comment Summary:
Another commenter stated that the Commission should remove “as a minimum” in 10 CFR 73.55(n)(2) because it is open to interpretation.

NRC Response:
The Commission disagrees. The Commission has determined that the phrase "as a minimum" is appropriate and has retained this phrase in the final rule. The Commission has concluded that 24 is a minimum, with more frequent reviews to be conducted when certain conditions exist.

Comment Summary:
One commenter stated that the proposed 10 CFR 73.55(n)(2)(ii) is open to interpretation and contains more restrictive requirements than those that currently exist. In particular, the commenter suggested that the Commission remove the phrase “but not be limited to” and replace the phrase “safety/security interface” with “plant operations/security interface.”

NRC Response:
The Commission disagrees. The Commission requires that the physical protection program be reviewed at intervals not to exceed every 24 months. The components listed in this requirement are all components of the physical protection program and, therefore, are applicable. Where licensee programs outside the security organization provide an appropriate review of these security-related programs, the licensee may take credit for that review provided its effectiveness as it pertains to the physical protection program is documented. The licensee is responsible to ensure that all elements the program are reviewed.

Comment Summary:
Another commenter suggested that the assessment process outlined in NEI 04-04 meets the requirement in 10 CFR 73.55(n)(2)(ii). The commenter suggested that the Commission add the clarifying language from NEI 04-04 to the SOCs. The commenter also suggested that the Commission clarify the SOCs to state that a single audit of a fleet level program will be sufficient to meet the requirement of each individual plant in that fleet.

NRC Response:
The Commission disagrees. The Commission has determined that the recommendation to include descriptions prescribed by industry guidance in the SOCs for this final rule is not appropriate. In addition, the Commission has also concluded that including a statement regarding the acceptability of a licensee audit process in the Statements of Consideration for this final rule is also not appropriate. Commission requirements apply to all sites regardless of corporate ownership of multiple sites.

Comment Summary:
One commenter stated 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.

NRC Response:
The Commission disagrees. The Commission has determined that this comment is outside the

scope of security program reviews and is addressed by the final rule in 10 CFR 73.54. The Commission has moved all cyber security program requirements from the proposed 10 CFR 73.55(m) to a stand-alone section 10 CFR 73.54, and therefore, has deleted this requirement from the final rule.

Comment Summary:
Another commenter stated that the assessment process outlined in NEI 04-04 meets the requirement in 10 CFR 73.55(n)(4). The commenter suggested that the Commission add the clarifying language from NEI 04-04 to the SOCs.

NRC Response:
The Commission disagrees that text from industry guidance should be incorporated into this rulemaking. The Commission's expectation is that the cyber security program is a component of the physical protection program and, therefore, must be reviewed at least every 24 months.

Comment Summary:
A third commenter stated that the proposed 10 CFR 73.55(n)(4) places cyber security within the licensees' security organization. The commenter suggested that since the current security organization does not currently oversee cyber security, the proposed 10 CFR 73.55(n)(4) is more appropriate under the proposed 10 CFR 73.58, or another new section.

NRC Response:
The Commission disagrees. The Commission's expectation is that the cyber security program is a component of the physical protection program and, therefore, must be reviewed at least every 24 months. This requirement does not specify the personnel to be used except that assigned personnel possess the requisite technical skills and knowledge needed to perform such a review.

Comment Summary:
One commenter asked for more detail on how the proposed rule addresses the expanded FOF requirements from the EPAct of 2005. In particular, the commenter asked about exercise periodicity and the rule text addressing potential conflicts of interest.

NRC Response:
The Commission has deleted this requirement from the final rule 73.55 because it is redundant to the final rule Appendix B, to Part 73. The requirements of Appendix B address the annual periodicity requirement and requirements for avoidance of conflicts of interest.

Comment Summary:
Another commenter noted that the proposed 10 CFR 73.55(n)(5) would require drills and exercises to be performed in accordance with the proposed new requirements in Part 73, Appendix C. The commenter suggested, however, that the requirements in proposed Part 73 Appendix C, Section II (l) through (l)(6)(iv) do not belong in the SCP. The commenter suggested that NRC reword 10 CFR 73.55(n)(5) to state that licensees conduct quarterly drills and annual FOF exercises in accordance with the performance evaluation program, as described in the Commission-approved security plans.

NRC Response:
The Commission disagrees. NRC requirements are addressed in the regulations and not by license security plans. However, the Commission has determined that this requirement is

redundant to the final rule Appendix B to Part 73 and, therefore, has deleted this requirement from the final rule 73.55.

Comment Summary:
Another commenter suggested that the Commission delete 10 CFR 73.55(n)(5) because it is not an audit or review requirement.

NRC Response:
The Commission agrees and has deleted this requirement from the final rule.

Comment Summary:
One commenter stated that the NRC should delete 10 CFR 73.55(n)(6) because requirements in subsequent provisions address corrective action programs (CAPs) adequately to address review and audit findings.

NRC Response:
The Commission disagrees. The Commission has determined that this requirement establishes the appropriate regulatory framework for the inclusion of security findings in the site's CAP.

Comment Summary:
One commenter stated that the NRC does not need to include 10 CFR 73.55(n)(8) in the final rule. The commenter explained that issues placed into the CAP are resolved within that program.

NRC Response:
The Commission agrees. The Commission has deleted this proposed requirement from the final rule. The Commission's expectation is that each license will make all appropriate changes to ensure the effectiveness of the physical protection program to meet NRC requirements and provide high assurance.

Comment Summary:
A commenter stated that audits are not annual, as suggested by the proposed rule. The commenter explained that audits are biennial, instead, and the proposed rule language should reflect that. Also, the commenter stated that NEI 03-12 provides the following guidance: audits may be conducted up to six months before or up to six months after the scheduled date. The next scheduled date is 24 months from the originally scheduled date.

NRC Response:
The Commission agrees in part. The Commission has deleted this requirement because the timeframes described are not appropriate to audits and reviews. The Commission uses the term "review" to mean a complete evaluation of all physical protection program components to confirm compliance with NRC requirements and the term "audits" to mean a component of reviews to confirm that the licensee is in fact following its internal plans, procedures, and policies.

Comment Summary:
One commenter asked who determines the "predetermined intervals" in which testing and maintenance are required. The commenter asked if the Commission plans to identify the predetermined intervals in guidance and whether the public will be able to comment on the

proposed interval. The commenter also asked if a piece of equipment fails to work, but this is discovered when the piece of equipment is not in operation, then is this failure considered a violation.

NRC Response:
This requirement provides generic performance-criteria for all physical protection program systems and equipment. The specific pre-determined intervals must be sufficient to maintain the equipment in operable condition and ensure that it is capable of performing its intended function. Generally, manufacturer specifications are considered appropriate. If not in use at the time of failure, this requirement does not apply.

Comment Summary:
A commenter asked the Commission, “Who defines or determines what is ‘security-related components or equipment?’”

NRC Response:
Each licensee determines “security-related components or equipment" through site-specific analysis and NRC regulations.

Comment Summary:
One commenter suggested that the NRC move 10 CFR 73.55(o)(1)(iv) to 10 CFR 73.55(p).

NRC Response:
The Commission disagrees. The NRC has determined that the focus of this requirement is failures associated with maintenance, testing, and calibration activities. The requirements of the final 10 CFR 73.55(o) provide performance-criteria to be met by compensatory measures.

Comment Summary:
Two commenters stated that intrusion detection and access control equipment referenced in the proposed 10 CFR 73.55(o)(3) are physical protection intrusion detection and access control equipment, and passwords are not considered a part of “access control equipment.” The commenters suggested that the Commission include clarification in the SOC to better define when the Commission is referring to physical access controls as opposed to electronic access to digital assets.

NRC Response:
The Commission agrees. This requirement focuses on the need for testing the “equipment” that physically controls access and does not include the testing of access control devices. The Commission disagrees that this distinction is necessary in the statements of consideration for this rulemaking.

Comment Summary:
One commenter stated that on-site and off-site communication systems should be tested no less than daily, and this requirement should never be relaxed.

NRC Response:
The Commission agrees with this comment specific to the requirement stated in the final 10 CFR 73.55(n)(5).

Comment Summary:
Another commenter suggested that the proposed 10 CFR 73.55(o)(5) is a new requirement. To remove the new requirements from the final rule, the commenter suggested that the Commission delete “each control room, and between the alarm stations and offsite support agencies.”

NRC Response:
The Commission disagrees. This requirement is retained from the pre-existing 10 CFR 73.55(g)(3) and is updated to clarify the entities with which this communication capability must be verified and maintained on a daily basis to support the physical protection program.

Comment Summary:
One commenter suggested that the NRCstaff replace the words “time lines” with “time frames.

NRC Response:
The Commission agrees. The term "time-lines" is most commonly used to describe actions required within licensee protective strategies and to avoid confusion, the NRC has revised the final rule to use the term "times-frames'.

Comment Summary:
One commenter suggested that the NRC rename this proposed 10 CFR 73.55(q) to “Suspension of security measures.” The commenter also suggested that the NRC change “safeguards measures” in 10 CFR 73.55(q)(1)(i) to say “security measures.”

NRC Response:
The Commission agrees.

Comment Summary:
A second commenter stated that the proposed 10 CFR 73.55(q)(1)(i) does not recognize the ISFSI safeguards suspension allowances authorized under 10 CFR 72.32(d). The commenter suggested that the Commission should incorporate the suspension allowances authorized under 10 CFR 72.32(d) in the final rule.

NRC Response:
The Commission disagrees. The Commission has determined that ISFSIs are addressed by other NRC regulations and, therefore, are not addressed herein.

Comment Summary:
A commenter suggested that the Commission change the word “safeguards” in 10 CFR 73.55(q)(1)(ii) to “security measures.” In this same provision, the commenter suggested that the Commission change “the security supervisor” to “security supervision.”

NRC Response:
The Commission agrees in part. The Commission agrees that the phrase "affected security measures" is more appropriate and has revised the final rule. The Commission disagrees with the suggested use of "security supervision" and has determined that the term “supervisor or manager” is needed to specify this individual.

Comment Summary:
Another commenter suggested that the proposed 10 CFR 73.55(q)(1)(ii) requires suspension

approval by a Senior Reactor Operator (SRO). The commenter stated that this requirement goes beyond the current Commission-approved security plan requirements as specified in NEI 03-12, "Template for the Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, [and Independent Spent Fuel Storage Installation Security Program]." The commenter suggested that the Commission revise this provision to require that the on-shift operations manager approve the suspension of safeguards, rather than a SRO.

NRC Response:
The Commission disagrees in part. The Commission has concluded that this allowance is based upon the current 10 CFR 50.54(x) and (y) and, therefore, must be approved by an individual who is in a position of management and who possesses an appropriate level of knowledge and understanding pertaining to the plant condition at the time that safeguards measures are suspended. The NRC-approved security plans, approved on October 26, 2004, specified the Emergency Director (who is generally the SRO or someone with equal knowledge and understanding) and Security Supervisor for this decision.

Comment Summary:
A commenter suggested that the NRC replace "reimplemented" in 10 CFR 73.55(q)(2) with "restored."

NRC Response:
The Commission agrees in part. The NRC has determined that the term reinstate is most appropriate.

Comment Summary:
A commenter suggested that the NRC change "safeguards measures" in 10 CFR 73.55(q)(3) to say "security measures."

NRC Response:
The Commission agrees.

Comment Summary:
A commenter suggested that the Commission move 10 CFR 73.55(q)(4) to the end of 10 CFR 73.55(q)(3).

NRC Response:
The Commission agrees. The NRC has deleted this requirement from this section.

Comment Summary:
A second commenter stated that 10 CFR 73.55(q)(4) appears to waive the requirement for duplicate reports under 10 CFR 50.72 only with respect to the suspension of safeguards measures. The commenter asked if this is the Commission's intent. The commenter continued that if it is the Commission's intent to waive all duplicate reports, then the NRC should move the requirement to 10 CFR 73.71.

NRC Response:
The Commission agrees. The NRC has determined that 10 CFR 73.71 addresses this requirement and, therefore, has deleted this requirement from the final rule.

Comment Summary:
One commenter asked what the difference is between 10 CFR 73.55(r)(1) and 10 CFR 73.55(d)(5)(ii). The commenter suggested that, if there is no difference, the NRC should delete 10 CFR 73.55(r)(1) from the final rule.

NRC Response:
Both requirements were retained from the current 10 CFR 73.55(b)(1)(ii). 10 CFR 73.55(r)(1) is retained and applies to the licensee. The requirement stated in 10 CFR 73.55(d)(5)(ii) applied only to a written statement that would be documented in a contract for security services. The Commission has determined that such a requirement to specify Commission regulations in a contract for security services is not necessary and therefore, has deleted 10 CFR 73.55(d)(5)(ii).

Comment Summary:
In the proposed 10 CFR 73.55(d)(5)(ii), one commenter recommended the NRC delete the words “copies of” from the provision, as the commenter did not believe it is necessary for the NRC to have original versions of reports.

NRC Response:
The Commission disagrees. The NRC has deleted the phrase "copies of" from the final rule to explicitly specify the Commission’s authority to remove originals or copies of any and all documents or records that are required by NRC regulations, whenever the Commission determines that such action is necessary.

Comment Summary:
Another commenter suggested that the proposed 10 CFR 73.55(r)(2) exceeds the current rule and security plan requirements. The commenter suggested that the Commission reword the final rule language to state that licensees must retain all records “in accordance with Commission-approved security plans.”

NRC Response:
The Commission disagrees with the suggested text because licensees retain records in accordance with Commission regulations and not security plans.

Comment Summary:
One commenter suggested that the NRC delete 10 CFR 73.55(s) of the proposed rule. The commenter explained that the NRC duplicates this section in 10 CFR 73.58.

NRC Response:
The Commission agrees. This Commission has deleted this proposed requirement because the applicable regulatory framework is established in 10 CFR 73.58.

Comment Summary:
A second commenter stated that the requirements in proposed 10 CFR 73.55(s) and 73.58 are unclear because the Commission does not explain what, if anything, is needed beyond current processes (e.g., site program impact process). The commenter suggested that the Commission expand the SOC section to explain the expectations for such a process, including what specifically is needed beyond current practices and procedures.

NRC Response:

The Commission agrees. This NRC has deleted this proposed requirement because the applicable regulatory framework is established in 10 CFR 73.58. The intent of this requirement was to provide a regulatory link between 10 CFR 73.55 and 73.58 and to emphasize the coordination of safety and security activities in a coherent manner.

Comment Summary:
In reference to proposed 10 CFR 73.55(a)(4), 73.55(c)(1), and 73.55(t)(2), one commenter noted that "the first reference states that licensees will implement the physical protection program in accordance with Commission regulations, etc., and the second reference appears to support that. However, the second reference acknowledges that alternative measures could be submitted in accordance with 10 CFR 50.4 and 50.90 and, therefore, might be approved by the Commission." The commenter asked: "What is the legally controlling document, the regulations or the licensees' NRC-approved physical security plans?"

NRC Response:
The Commission concluded that this comment may reflect an over simplification of the NRC regulatory processes. It is more accurate to state that both the NRC's regulations and the NRC-approved plans are legally controlling, however, the fact that a licensee has an NRC-approved security plan does not relieve the licensee from compliance with NRC regulations. NRC regulations are legally controlling in that they set forth the regulatory framework and general performance objectives and requirements to be implemented by each licensee. The NRC-approved plans describe how the licensee will comply with NRC regulations through implementation, which ***includes*** any NRC-approved exemptions and alternatives. To the extent that there are differences between the licensee's security plan and NRC requirements, those differences must be explicitly approved by the NRC, through an NRC-granted exemption (10 CFR 73.5), or an NRC-approved "alternative measure" (final rule 10 CFR 73.55(r)).

The Commission recognizes that generic regulations cannot always account for site-specific conditions and, therefore, has determined that some degree of regulatory flexibility is necessary to ensure that each licensee is able to design their physical protection program to effectively satisfy the "high assurance" performance objective in the final rule (10 CFR 73.55(b)). Therefore, the final rule is revised to address the mechanisms through which the Commission reviews and approves a licensee's need for an alternative measure or exemption from one or more NRC requirements provided sufficient justification is demonstrated.

Upon the NRC's written approval, the measure or measures specified by the NRC in writing, become legally binding as a license condition in lieu of the specific requirement stated in the regulations. It is important to note that the fact that the NRC may have approved a security plan containing a deficiency or conflict, does ***not*** shield the licensee from regulatory compliance. In such cases the NRC and licensee will work together to resolve the conflict and if needed, changes could be made to the licensee's security plans to ensure all Commission requirements are met.

Comment Summary:
One commenter suggested that the Commission reword 10 CFR 73.55(t)(4) so that it says, "vehicle barrier systems alternative to those required by 10 CFR 73.55(e)(8)," rather than "alternative vehicle barrier systems required by 10 CFR 73.55(e)(8)".

NRC Response:
The Commission agrees in part. The NRC has revised final rule text.

Comment Summary:
Regarding 10 CFR 73.55(t)(4)(i), one commenter stated that the term ‘vehicle bomb’ is too limiting. The commenter asked, “What if, instead of a bomb, the vehicle itself is used to cause the damage?” The commenter believes the Commission should delete the term ‘bomb’ from this section.

NRC Response:
The Commission agrees in part. The NRC has revised the final rule text consistent with 10 CFR 73.55(e)(8)(i) and 73.55(e)(8)(iv) for protection against the use of a vehicle as a means of transportation.

10 CFR 73.56
Responses to Public Comments

Comment Summary:
One commenter argued that the proposed Power Reactor Security Requirements Rule was utterly inadequate and that it was clear that the Commission had drawn the line at the point where nuclear power operators' profit margins might be significantly affected. This commenter noted that terrorists do not have such a constraint. He suggested that, if the Commission does not believe its licensees can afford the security upgrades necessary to protect the nation's nuclear reactors against the full potential threat, it must act with forthrightness and publicly demand that the Department of Homeland Security or the U.S. military assume responsibility for domestic nuclear power plant security. This commenter made several points that dealt with how terrorists could gain access to nuclear power plants and the very real threat that "insiders" pose.

NRC Response:
The Commission disagrees with the commenter regarding the NRC beliefs about the licensees' ability to afford the security needed to protect the nation's nuclear reactors and the public health and safety and the common defense and security and disagrees with the commenter's contention that the NRC should demand that either the Department of Homeland Security or the U.S. military should assume responsibility for domestic nuclear power plant security. The Commission is aware that changes in security requirements will have varying degrees of expense. However, the Commission does believe that licensees subject to this rule are able to make the changes that are needed and that the benefits to the licensees, as well as to the public health and safety and the common defense, derived from the increased security will be well worth the cost of the changes.

Comment Summary:
One commenter, supported by many other commenters, stated that the proposed 10 CFR 73.56(a)(1) requirement that each licensee submit its amended access authorization program to the NRC for review and approval would be a new requirement that goes beyond the requirements in the Access Authorization Order, dated January 7, 2003. That order allows each licensee to certify to the NRC that it has implemented an access authorization program that meets the NRC requirements. The commenter argued that a licensee should be allowed to certify to the NRC that its program is consistent with or exceeds the NRC-approved generic authorization program. This would result in significant resource savings for both the NRC and licensees and allow licensees to implement the amended program much earlier.

NRC Response:
The Commission agrees with that each licensee can certify to the NRC that it has implemented an access authorization program that meets the NRC's requirements. The Commission finds that 10 CFR 50.54 or 10 CFR 50.90 provides regulations regarding whether the licensees are required submit changes to their Physical Security Plan. Therefore, the Commission has deleted the requirement in the proposed rule for each licensee to submit its amended program for NRC review and approval.

Comment Summary:
One commenter, supported by many other commenters, stated that proposed 10 CFR

73.56(a)(6) did not make clear that only licensees and applicants can deny individuals access to a particular site. The commenter recommended that this proposed provision be revised to clearly state that, while licensees, applicants, and contractors/vendors should be able to maintain individuals' unescorted access authorization only licensees and applicants should be permitted to grant individuals unescorted access (UA) to their own nuclear power plant protected and vital areas, maintain such access, or deny such access.

NRC Response:
The Commission agrees with the comments that the authority over an individual's unescorted access to the protected and vital areas of a site is held only by that site's licensee. The Commission also agrees that greater clarity is needed about the relative roles and authorities of licensees and applicants versus contractor/vendors with regard to the access authorization programs and access determinations required by this rule. Therefore, the NRC has revised Section 73.56(a)(4) to make clear that only a licensee has the authority to grant unescorted access an individual.

Additionally, the Commission has revised Paragraph 73.56(a)(4) to allow both licensees and applicants to certify an individual unescorted access authorization and to permit to maintain, deny, terminate, or withdraw unescorted access authorization status. Although contractors or vendors do not have authority to grant or certify an individual unescorted access or unescorted access authorization, they can complete the access authorization program elements for licensees or applicants. Additionally, the contactors or vendors may maintain individuals' unescorted access or unescorted access authorization on behalf of the licensees and applicants, if the contractor access programs include the licensees or applicants approved behavior observation program. Because the licensees and applicants rely on the contractors and vendors to comply with the requirements of this section, the contractor access programs must comply with the requirements of this section.

Comment Summary:
One commenter, supported by many other commenters, stated that proposed 10 CFR 73.56(b) did not allow for short-term escorted digital access. The commenter noted that the industry presumes that defined permissions for supervised digital access for designated vendors/consultants are allowed in the same spirit as escorted physical access. The commenter argued that it is not practical to process all short-term computer support personnel through the access authorization program, and recommended that the rule allow these individuals to provide their expertise on a short-term, supervised basis.

NRC Response:
The Commission finds that the received comment regarding electronic escorted access is 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 plant. Therefore, the Commission did not revise the rule text.

Comment Summary:
One commenter, supported by other commenters, noted that licensees have no way to control access to off-site emergency response components that include commercial facilities, such as telephone switch stations, and that proposed 10 CFR 73.56(b) should be revised to reflect this.

NRC Response:
The NRC finds that the received comment is 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.

Comment Summary:
One commenter, supported by many other commenters, stated that proposed 10 CFR 73.56(d)(1)(i)(B) assumes all contractors/vendors have access to information through the information-sharing mechanism required under the proposed 10 CFR 73.56(o)(6). The commenter noted that the information-sharing mechanism has functioned for many years with approximately twelve contractors/vendors having access. Because the access decision for power reactor protected areas rests solely with the licensees, there is no reason for all contractors/vendors to have such access. The commenter recommended that the proposed 10 CFR 73.56(d)(1)(i)(B) be reworded to say that licensees "will," but applicants and contractors/vendors "may" (as opposed to "will"), have access to information documenting the withdrawal through the information-sharing mechanism.

NRC Response:
The Commission agrees with the comments and has revised the proposed rule text in the final rule to reflect the received comments. As discussed in the response to comments received on proposed paragraph (a)(4), the term "applicant," or "applicants," in this section means only those applicants who have chosen to implement their access authorization program that comply with requirements set forth in this section prior to receiving their operating licenses or their NRC findings or nuclear fuel. Additionally, as explained in Paragraph (a) of this section, the term "contractors or vendor" means any entity or person as defined in 10 CFR 50.2 who maintains a contractor or vendor authorization program that has been approved by a licensee or an applicant who uses the contractor or vendor to complete its access authorization program elements that comply with requirements set forth in this section. These contractors or vendors may have access to information-sharing systems.

The Commission agrees that contractors or vendors may have access to the information sharing mechanism. Therefore, to provide additional clarifications, the Commission has revised the final rule text to state that the contractors or vendors may have the same access to the information, if such information is necessary to assist licensees or applicants to comply with the requirements set forth in section. Additionally, the Commission revised throughout the entirety of the final rule text to ensure that it does not inadvertently suggest that all contractors or vendors are required to access the information-sharing mechanism.

Finally, the Commission's explanation of the term "applicant" or "applicants", above, applies in response to all of the comments received on the proposed rule.

Comment Summary:
One commenter, supported by many other commenters, noted that when an individual withdraws his or her consent for a background investigation, the industry does not record the reason for the withdrawal in its information sharing mechanism because the reason is not pertinent for any access determination. Therefore, the commenter recommended deleting the proposed 10 CFR 73.56(d)(1)(ii) requirement that the individual's reason for withdrawing consent be recorded in the information sharing mechanism. The commenter also noted that contractors and vendors currently do not have data entry capabilities for the data-sharing mechanism.

NRC Response:

The Commission agrees with the received comment that access authorization status information is recorded in the information sharing mechanism, instead of collected records. Additionally, the Commission agrees with the commenters regarding contractors or vendors accessing the information sharing mechanism. The intent of the proposed rule was not to require all contractors or vendors to directly input or update records in the information sharing mechanism. However, the contractor or vendor may assist licensees or applicants if assistance is requested by them. Therefore, the Commission revised the final rule text to require that the status of individual's application for access authorization for licensees or applicants is recorded to the information sharing mechanism accordance with Paragraph o(6) of this section.

Comment Summary:
One commenter, supported by many other commenters, recommended that proposed 10 CFR 73.56(d)(2)(ii) be deleted from the final rule. They noted that, currently, licensees indicate administrative withdrawals in the information-sharing mechanism. This prevents the individual from beginning the access authorization process at another licensee until that licensee communicates with the licensee who indicated the administrative withdrawal.

The commenter also noted that the licensee that originally entered the administrative withdrawal indication removes it from the information sharing mechanism when appropriate. If the individual is subsequently denied or terminated unfavorably, that information is entered in the information-sharing mechanism and the administrative withdrawal indication is removed. The commenter claimed that there was no need for the proposed 10 CFR 73.56(d)(2)(ii) requirement because all administrative withdrawal indications are removed from the information-sharing mechanism when appropriate. He also expressed concern that the Commission was attempting to prescribe very specific requirements that are contrary to the logical functioning of the information sharing mechanism that has been developed, tested, and proven over the last decade.

NRC Response:
The NRC agrees with the comments that licensees remove administrative withdrawal indication from the information-sharing mechanism, when appropriate. However, the NRC finds that the final rule text must maintain the intent of the former rule that addresses concerns regarding inadvertent sharing of information that is no longer applicable to an individual who is seeking unescorted access at a nuclear facility. Therefore, the Commission has revised the final rule text to incorporate the comment and maintain the intent of the former rule.

The Commission finds that the current industry practice to share a temporary or administrative state of individuals' access authorization status among licensees, applicants, and contractors or vendors is a necessary part of access authorization program. However, the NRC also is concerned that old or stale information that is no longer applicable to the individual would inadvertently be shared. Therefore, the NRC has revised the final rule text to maintain the intent of the original language and preserve the industry's current practice.

Comment Summary:
One commenter, supported by many other commenters, stated that proposed 10 CFR 73.56(d)(3) did not fully address the legal avenues that foreign nationals have for performing work supporting licensees in the United States. For example, under the North America Free Trade Agreement (NAFTA), Canadians performing certain services for a Canadian-based company require neither an alien registration nor an I-94 Form to be in the United States legally.

For certain Federal government databases, immigration status verification cannot be performed without an alien registration number or an I-94 Form. Additionally, many contract workers supporting licensees require access either the day of or the day after arriving in the United States. All aliens are issued an admission number when they enter the United States. But processing of I-94 Form paperwork by the Federal government often does not yield an immigration status validation result until up to 10 business days following the worker's arrival in the United States.

The commenter suggested that the proposed 10 CFR 73.56(d)(3) be revised to require licensees and applicants to validate the "the claimed immigration status" rather than "the alien registration number that the individual provides." The commenter also recommended that contractors and vendors be eliminated from proposed 10 CFR 73.56(d)(3) because, as provided in proposed 10 CFR 73.56(a)(6), contractors and vendors do not grant unescorted access. Also, the commenter noted that proposed 10 CFR 73.56(d)(3) incorrectly referred to fingerprinting being required under 10 CFR 73.21.

NRC Response:
The Commission agrees with the received comments regarding claimed immigration status. NAFTA allows Canadians performing certain services to enter the United State without either an alien registration or an I-94 Form. Additionally, the Commission agrees with the commenters that the proposed rule text incorrectly allowed contractors or vendors to evaluate the results of fingerprinting required under 10 CFR73.56. Although contractors or vendors may conduct local criminal history check, Section 149 of Atomic Energy Act prohibits them from evaluating the results of fingerprinting required under 10 CFR part 73.57. Finally, the NRC agrees with the commenters that the proposed rule incorrectly references 10 CFR 73.21. Therefore, the NRC has revised the proposed rule text in the final rule to cover foreign nationals who entered the United States under NAFTA, to correct errors in referencing fingerprinting requirements, and to delete contractors or vendors from evaluating the criminal history records obtained in accordance with 10 CFR 73.57.

Comment Summary:
One commenter, supported by many other commenters, stated that proposed 10 CFR 73.56(d)(4)(iii) went beyond the requirements of the Access Authorization Order, dated January 7, 2003. The commenter stated that the industry's experience indicates that compliance with proposed 10 CFR 73.56(d)(4)(iii), requiring the licensee, applicant, or contractors/vendors to verify that an individual had actively participated in the education process would be difficult at best and, at times, impossible. Thus, the commenter recommended that the Commission revise 10 CFR 73.56(d)(4)(iii) by replacing the phrase "verify that the individual was actively participating in the education process during the claimed period" with "verify that the individual was actually registered for class during the claimed period".

NRC Response:
In general, the Commission agrees with the commenters that verifying that an individual had actively participated in the education process would be difficult. The intent of this requirement was for licensees, applicants, and contractors or vendors to verify that the individual who applied for either unescorted access or unescorted access authorization was registered for the classes and received grades that indicate that the individual actively participated in school during the claimed period(s). Therefore, the Commission has revised the proposed rule text in the final rule to reflect the intent of this rule.

Comment Summary:
One commenter, supported by many other commenters, stated that the proposed 10 CFR 73.56(d)(4)(vi) was more stringent than the related requirements in the Access Authorization Order, dated January 7, 2003. The commenter interpreted 10 CFR 73.56(d)(4)(vi) to require that licensees, applicants, and contractors/vendors must keep all documents gathered during the employment history evaluation. The commenter noted that this paragraph referred to the proposed 10 CFR 73.56(o), and that 10 CFR 73.56(o)(2)(i) and (ii) clearly required retention of only those records actually used in the access determination. The commenter recommended that the Commission revise 10 CFR 73.56(d)(4)(vi) to make it consistent with the more limited requirements of 10 CFR 73.56(o)(2)(i) and (ii).

NRC Response:
The NRC disagrees with the comment that the recordkeeping requirement set forth in this paragraph is inconsistent with 10 CFR 73.56(o) and 10 CFR 73.56(o)(2)(i). The proposed rule text specifically requires licensees, applicants, or contractors or vendors to retain the records and any documents or electronic files obtained electronically. Additionally, this requirement is consistent with related requirements in 10 CFR Part 26.

Comment Summary:
One commenter, supported by many other commenters, said that the industry did not take issue with proposed 10 CFR 73.56(d)(5) that required an evaluation of the credit history of an individual applying for access. The commenter noted, however, that it is important to recognize that information in credit reports provided by credit reporting agencies may not agree with information provided by individuals. Given this potential for inconsistency, he thought that reviewing officials should use data provided by credit reporting agencies in the context of the other information developed during the access process.

Also, the commenter stated that proposed 10 CFR 73.56 had no requirement for evaluating the credit history of a foreign national and suggested that the rule require a financial responsibility inquiry for unescorted access authorization applicants with a residence of record in a foreign country and who have not established a record of credit in the United States.

The commenter further suggested that, if no routinely accepted credit reporting mechanism is available in the applicant's country of recorded residence, a statement of responsibility concerning the individual's financial record from an entity within that country should be considered acceptable.

In addition, the commenter argued that the term "full credit history evaluation" was ambiguous. He recommended that the NRC delete the word "full" and specify a required specific credit history time period for industry to use and provide justification for it. Lastly, the commenter noted that fraud checks are not available from the national credit-reporting agencies.

NRC Response:
The Commission agrees in part with the comments. The Commission agrees with the comments that the information in credit reports may not match the information provided by individuals and that the reviewing official should interpret the credit history information within the context of all the information developed during the access authorization process. This is consistent with the Commission's intent.

The Commission also agrees that the credit history of foreign nationals and individuals without

an established credit history in the United States should be evaluated, and that multiple sources could potentially provide information about an individual's financial record and responsibility, including, but not limited to, routinely accepted credit reporting mechanisms. Thus, the NRC has revised the final rule text to provide requirements for individuals, such as foreign nationals and United States citizens who have resided outside the United States, who have not established credit history in the United States.

However, the Commission disagrees with the commenter concerning the benefit and feasibility of conducting full credit history evaluations and the role of credit history information in identifying patterns of fraud and misuse of financial identifiers. Additionally, the Commission disagrees with the recommendation that the regulations should specify and justify a specific time period for credit history evaluation. The NRC issued additional clarification regarding a full credit history check in Regulatory Issue Summary 2005-14, "Clarification of implementing Guidance for Compensatory Measures Related to Access Authorization".

This full credit history evaluation is consistent with current industry practice. The full credit history evaluation requirement reflects the Commission's intent that all financial information available through credit-reporting agencies is to be obtained and evaluated. Experience has shown that the information available from credit sources varies in the time period covered, depending upon the individual and the information source. Because these records can reveal patterns of fraud or misrepresentation that are of particular value in assessing an individual's trustworthiness and reliability, the Commission has concluded that it is important to obtain and evaluate all available information of this type.

The Commission also disagrees with the commenter's interpretation that the proposed rule indicates that credit reporting agencies conduct fraud checks. Rather, the Commission is making the point that evaluation of information obtained through a request for a full credit history on an individual may reveal fraud and misrepresentation or misuse of financial identifiers.

Comment Summary:
One commenter, supported by many others, stated that proposed 10 CFR 73.56(e)(1) required that a clinical psychologist or psychiatrist conduct the psychological assessment. The commenter assumed the rule's intent was to ensure that the individual performing the professional work was properly trained and experienced in conducting psychological assessments. However, he reported that a sample of state licenses for psychologists found no states that specifically licensed "clinical psychologists." Therefore, the commenter recommended that proposed 10 CFR 73.56(e)(1) be revised to specify that psychological assessments be conducted by a psychologist who has adequate experience, rather than the more specific requirement of a clinical psychologist.

NRC Response:
The Commission agrees with assumption that intent of the rule was to ensure that the individual performing the professional work was properly trained and experienced. Additionally, the NRC agrees with the commenter that some states license psychologists or psychiatrists instead of clinical psychologists or psychiatrists. Therefore, the Commission revised the final rule text to require "a licensed psychologist or psychologist with the appropriate training or experience" to conduct the psychological assessment.

Comment Summary:
One commenter, supported by many other commenters, stated that proposed 10 CFR

73.56(e)(2) required that psychological assessments be conducted in accordance with the applicable ethical principles established by the American Psychological Association or American Psychiatric Association. The commenter noted that the Commission discussion recognized that, to meet state licensure requirements, clinical psychologists and psychiatrists are required to practice in accordance with applicable professional standards but did not require that clinical psychologists and psychiatrists practice in accordance with American Psychological Association or American Psychiatric Association ethical principles. The commenter stated that the industry was concerned that licensees may not be able to use licensed and fully qualified clinical psychologists and psychiatrists because their practices, while ethical, deviate slightly from the ethical principles of the relevant association. The commenter concluded that it would be inappropriate for the Commission to mandate that any professional practice adhere to a cannon of ethics which might deviate from the demands of the State Board that granted their license. Thus, the commenter recommended that the Commission revise 10 CFR 73.56(e)(2) to state that the psychological assessment must be conducted in accordance with the applicable ethical principles for conducting such assessments established by the State Board granting licensure to the psychologist or psychiatrist.

NRC Response:
The NRC disagrees with the comments because the ethical principles established by the American Psychological Association or American Psychiatric Association address the issues raised by the comments. Specifically, these ethical standards require psychologists and psychiatrists to comply with the requirements of laws, regulations (including requirements in Section 73.56), or other governing legal authorities. Thus the Commission finds that the requirements set forth in this section will not limit the pool of available licensed and qualified psychologists and psychiatrists who can perform the required psychological assessments.

Comment Summary:
Another commenter stated that the requirement in 10 CFR 73.56(e)(2) that the professionals conducting the psychological testing follow both the American Psychological Association and American Psychiatric Association ethical principles may conflict with the requirement in proposed 10 CFR 73.56 (e)(3) that a face-to-face interview may be conducted only after an individual surpasses predetermined thresholds on a psychological test.

The commenter noted that in Section 9.02a on “Use of Assessments” of the American Psychological Association's June 1, 2003, version of its “Ethical Principles of Psychologists and Code of Conduct,” it is clear that “Psychologists administer, adapt, score, interpret or use assessment techniques, interviews, tests, or instruments in light of the research on or evidence of the usefulness and proper application of the techniques.” The commenter said that tests like the MMPI-2, California Personality Inventory, or the Personality Assessment Inventory were designed for broad use to detect psychopathology. The commenter questioned whether there is any research that supports the use of these types of tests in settings where the motivation to fake good is high. He also questioned whether there is any research to show a connection between these tests and job requirements like trustworthiness and reliability that might be necessary to avoid violating federal legal protections under the “Americans with Disabilities Act.”

Lastly, the commenter stated that Section 2.01 of the APA Ethical Principles stresses that psychologists perform work only for those purposes that they are trained and properly supervised. The commenter said that, while all clinical psychologists receive training in administering tests that detect psychopathology, not many are familiar with applying these tests in national security settings where they are being asked to show a connection between test

results and the concepts of “trustworthiness” and “reliability” that the Commission is primarily interested in. The commenter asked whether there is a training program or a certification process in place for licensed psychologists or psychiatrists doing these personnel screenings.

NRC Response:
The NRC disagrees with the commenter that the proposed requirements prevent the professionals providing psychological assessment services from conducting a clinical interview with an individual, because 10 CFR 73.56(e)(3) does not impose such a prohibition. Therefore, the Commission finds that 10 CFR 73.56(e)(3) is not in conflict with 10 CFR 73.56(e)(2).

In reference to the concern that there must be sufficient demonstrated ability of psychological tests to shed light on a person’s trustworthiness and reliability and to comply with the Americans with Disabilities Act standards, the Commission directs the commenter’s attention to the considerable body of research and the reasonably long track record of intelligence and other agencies using the MMPI-2 as well as other personality tests for this purpose. Additionally, psychological assessment is one of many access authorization program elements that licensees and applicant use for determining individual’s trustworthiness and reliability. Therefore, the Commission is confident that results of psychological testing and the results of other access authorization program elements will provide high assurance regarding individual’s trustworthiness and reliable.

Comment Summary:
One commenter, supported by many other commenters, stated that 10 CFR 73.56(e)(3) would create requirements beyond those of the Access Authorization Order, dated January 7, 2003. The commenter noted that the provision requires “predetermined thresholds” to be applied in interpreting the results of the psychological test. The commenter argued that it would be completely inappropriate for the industry to set a professional clinical threshold for test performance to determine whether an individual shall be interviewed by a psychiatrist or licensed clinical psychologist as the proposed 10 CFR 73.56(e)(3) appeared to require.

The commenter suggested that the psychiatrist or psychologist should 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 paragraph (e)(4)(i) of this section. Further, the commenter stated that in some cases the psychiatrist or licensed psychologist should be allowed to interview the individual without administering the test if, in the professional opinion of the psychiatrist or licensed clinical psychologist, the test would provide little meaningful information.

The commenter concluded that it is not appropriate for the Commission to dictate practice requirements for professionals licensed by the various states. Thus, the commenter recommended that the Commission revise 10 CFR 73.56(e)(3) by adding the clause “unless waived” after “the psychological assessment must.” Also, the commenter recommended that the NRC replace the second sentence in the proposed provision with “A psychiatrist or licensed psychologist may waive the test and proceed directly with the interview if in his opinion the test would provide little meaningful information”.

NRC Response:
The NRC agrees that the predetermined threshold for each scale should be applied to the test established by a licensed and appropriately trained and/or experienced psychologists or psychiatrists following the applicable ethical principles for conducting such assessments

established by the American Psychological Association or American Psychiatric Association. The psychologists or psychiatrists who conduct the psychological evaluations are expected to be skilled in the administration of the tests they are using and are expected to have the knowledge and experience to select or develop the thresholds that are pertinent and effective for the purposes of the evaluation and the population being evaluated.

Finally, the predetermined threshold for each scale must be applied equally and fairly to all individuals subject to the psychological assessment requirement. Thus the Commission does not agree that the psychologist or psychiatrist should be able to waive the test and proceed directly with the interview if the psychologist or psychiatrist documents his or her opinion that the test would provide little meaningful information.

Comment Summary:
Another commenter stated that it is not enough to simply have predetermined thresholds on a psychological test. The commenter stated that whoever does the psychological testing must also review individual test items that may be of concern and review a life history questionnaire completed by each individual. Based on answers to particular questions of concern the individual may need to be evaluated face-to-face, whether or not his scale score meets the predetermined threshold. Also, the commenter noted that the substantial variability in the thresholds used by authorization programs in the past to determine whether an individual's test results provided indications of personality disturbances or psychopathology is a significant concern.

The commenter argued that setting predetermined thresholds is only a partial solution. In his view, the best way to reduce this variability across programs is to ensure that all licensed psychologists and psychiatrists are adequately trained and/or certified in applying their clinical assessment knowledge to this arena where “trustworthiness” and “reliability” are important concepts that may mean different things to different clinicians.

NRC Response:
The NRC agrees that requiring predetermined thresholds is not a complete solution and may not produce consistency across licensee programs, but does expect that it will increase consistency in this aspect within a licensee’s program. Finally, the NRC agrees with the recommendation to reduce inconsistencies among programs by ensuring that all licensed psychologists and psychiatrists are adequately trained and/or certified in applying their clinical assessment knowledge to this arena where “trustworthiness” and “reliability” are important concepts that may mean different things to different clinicians. The recommended solution is consistent with the requirements set forth in Paragraph 73.56(e)(1) of the final rule text that requires licensed psychologists and psychiatrists to be properly trained.

Comment Summary:
One commenter, supported by many other commenters, stated that proposed 10 CFR 73.56(e)(5) would create requirements beyond those of the Access Authorization Order, dated January 7, 2003. The commenter argued that proposed 10 CFR 73.56(e)(5) was very limiting and prescriptive in that it would force the reviewing official to be the focal point for the discussion of medical-related information.

The commenter recommended that this section be modified because premature involvement of the reviewing official may cause problems, such as ensuring that the right information is communicated back and forth between the psychologist or psychiatrist and medical doctor,

which would require development of a documentation tool. The commenter stated that knowledgeable professionals should discuss the issues and provide a recommendation to the reviewing official. According to the commenter, licensees, applicants and contractors and vendors can develop a process to achieve this goal.

NRC Response:
The Commission agrees that the reviewing official may not need to be the focal point for the discussion of medical-related information. A knowledgeable professional may provide results of his or her evaluation and recommendations regarding the individual to the reviewing official. However while developing a response to the comments, the Commission recognized that the proposed rule does not provide clear regulations other than initial psychological testing. The Commission finds that in order to maintain high assurance that each person granted unescorted access to the protected and vital areas is trustworthy and reliable and does not constitute an unreasonable risk to the health and safety of the public or the common defense and security, the psychological assessment regulations need to include requirements for those individuals who are granted unescorted access to protected or vital areas or are certified unescorted access authorization.

For these individuals, the reviewing officials need to reassess their trustworthiness and reliability when the psychologist or psychiatrist discovers any information that can adversely impact the individual's fitness for duty or trustworthiness and reliability. Therefore, the Commission has added paragraph (e)(6) to provide requirements beyond initial psychological testing.

Comment Summary:
One commenter asked the Commission to revise 10 CFR 73.56(f) to provide specific guidance on if or how someone will be psychologically screened if his or her access is suspended or removed for, say, abnormal behavior reported under the behavioral observation program.

NRC Response:
The NRC disagrees with this comment. The Commission finds that such specific guidance is provided in the regulatory guide and/or plant procedures, not in the rule itself.

Comment Summary:
One commenter, supported by many other commenters, stated that 10 CFR 73.56(f)(3) would create requirements beyond those of the Access Authorization Order, dated January 7, 2003. The commenter objected to the 10 CFR 73.56(f)(3) requirement that individuals report concerns arising from behavioral observation, such as those related to any questionable behavior patterns or activities of others, to the reviewing official. The commenter questioned the NRC's justification for this requirement and reported that, in the industry's experience, it is much more likely that concerns reported to supervisors are, in fact, subsequently reported to the reviewing official than not reported.

In the commenter's view, this new requirement would actually reduce the number of concerns reported because individuals often do not know who the reviewing official is. Furthermore, the commenter thought that industry employees' increased security consciousness since September 11, 2001, has made them more conscientious about reporting such concerns. For these reasons, the commenter recommended that proposed 10 CFR 73.56(f)(3) be revised to allow individuals subject to access authorization programs to have the option of reporting such concerns to the reviewing official, their supervisor, or other management personnel, as specified in site procedures.

NRC Response:
The Commission agrees, in part, with the above recommendation. The Commission agrees that that individuals should be able to report their concerns arising from behavioral observations to the reviewing official, the individual's supervisor, or other management personnel designated in their site procedures. However, the Commission disagrees that individuals subject to access authorization programs only report their concerns to individuals specified in the site procedures.

The objective of this requirement is to ensure that the reviewing official is promptly informed of circumstances or conditions that may have the potential to have an adverse impact on the trustworthiness and reliability determination related to that individual. Thus any necessary action regarding the individual's access authorization can be taken without delay. The timely review of this information will ensure, to the degree possible, that the reported individual will not constitute an unreasonable risk to the public health and safety and the common defense and security. 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.

Therefore, the Commission has revised the proposed rule text in the final rule to allow individual to report their concerns arising from behavioral observations to supervisors or managers who have the responsibility to report the concerns to the reviewing official.

Comment Summary:
One commenter, supported by many other commenters, stated that 10 CFR 73.56(g) would create requirements beyond those of the Access Authorization Order, dated January 7, 2003. The commenter objected to the 10 CFR 73.56(g) requirement that individuals report to the reviewing official "…any formal action(s) taken by a law enforcement authority…to which the individual has been subject…." He questioned the Commission's justification for this requirement and reported that, in the industry's experience, it is much more likely that arrests or other legal actions reported to supervisors are, in fact, subsequently reported to the reviewing official than not reported. In the commenter's view, this new requirement would actually reduce the number of arrests reported because individuals often do not know who the reviewing official is. For these reasons, the commenter recommended that 10 CFR 73.56(g) be revised to allow individuals subject to access authorization programs to have the option of reporting such legal actions to either the reviewing official, their supervisor, or other management personnel, as specified in site procedures.

NRC Response:
The Commission agrees in part with this comment. The Commission agrees that that individuals should be able to report legal actions to the reviewing official, the individual's supervisor, or other management personnel designated in their site procedures. However, the Commission disagrees that individuals subject to access authorization programs only report their legal actions to the individuals specified in the site procedures.

The objective of this requirement is to ensure that the reviewing official is promptly informed of circumstances or conditions that may have the potential to have an adverse impact on the trustworthiness and reliability determination related to that individual. Thus any necessary action regarding the individual's access authorization can be taken without delay. The timely

review of this information will ensure, to the degree possible, that the reported individual will not constitute an unreasonable risk to the public health and safety and the common defense and security. 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.

Therefore, the Commission has revised the proposed rule text in the final rule to allow individual to report their legal actions to supervisors or managers who have the responsibility to report the concerns to the reviewing official.

Comment Summary:
Two people jointly commented that the 10 CFR 73.56(g) requirement that individuals who have applied for or are maintaining unescorted access authorization report to the reviewing official "any formal action(s) taken by a law enforcement authority" was overly broad and would set workers up for retaliation by management. The commenters noted that, at a public meeting, the NRC acknowledged that the intent of this provision did not apply to, for example, such minor infractions as speeding or parking tickets. However, proposed 10 CFR 73.56(g) itself did not exclude such minor infractions. The commenters concluded that this requirement could be abused by licensees in their campaign to rid workplaces of people raising safety concerns and that the Commission must not make it easier for its licensees to retaliate against workers who raise safety concerns.

NRC Response:
The NRC agrees with the commenters that the term "any formal action(s)" is overly broad and has revised 10 CFR 73.56(g) in the final rule to clarify that individuals subject to an access authorization program are required to report only legal actions that could result in incarceration or a court order or that require a court appearance, including but not limited to an arrest, an indictment, the filing of charges, or a conviction, but excluding minor misdemeanors such as parking or speeding tickets.

Comment Summary:
One commenter, supported by many other commenters, stated that some aspects of 10 CFR 73.56(h)(4) would create requirements beyond those of the Access Authorization Order, dated January 7, 2003. The commenter also noted that, while 10 CFR 73.56(h)(4) required licensees, applicants, and contractors/vendors to take actions as specified in physical security plans, the NRC-approved physical security plans do not direct specific actions for the access program. Rather they mention that access actions are to be taken in accordance with the industry standard access program, which sites have typically converted to their own access programs.

Thus, the commenter recommended that proposed 10 CFR 73.56(h)(4) be revised to provide that, if potentially disqualifying information is disclosed or discovered about an individual, action is to be taken in accordance with the licensee's or applicant's access program or implementing procedures rather than its physical security plan.

NRC Response:
In general, the Commission agrees with the comment. To increase clarity in the organizational structure of the requirements set forth in proposed paragraphs h(3), (h)(4), h(5), h(6), and (h)(7), the Commission combined those paragraph into (h)(4) in the final rule text. During this update, the Commission deleted the rule text concerning potentially disqualifying information that is

disclosed or discovered about an individual, because paragraph (h)(3) of the final rule provides regulation regarding the disclosed and discovered information. Specifically, paragraph (h)(3) of the final rule requires the licensee's or applicant's reviewing official to evaluate all of the information required by this section prior to granting an individual unescorted access or certifying an individual unescorted access authorization.

Comment Summary:
One commenter, supported by many other commenters, stated that some aspects of proposed 10 CFR 73.56(h)(8) would create requirements beyond those of the Access Authorization Order, dated January 7, 2003. The commenter also said that the industry agreed with the 10 CFR 73.56(h)(8) requirement that the decision to grant or maintain unescorted access authorization shall not be made until all of the required information has been provided to the reviewing official. The commenter stated, however, that the decision to deny or terminate such authorization should be made 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 10 CFR 73.56.

Additionally, the commenter noted that industry and the NRC have used the word "determination" to characterize this decision, but contrary to this established practice, the final sentence of proposed 10 CFR 73.56(h)(8) calls this decision a "positive finding." Thus the commenter recommends changing the terms to "determination of trustworthiness and reliability." The commenter also suggested revising this section so that it would apply to licensees and applicants but not to contractors and vendors.

NRC Response:
The Commission agrees with the comment that, if a reviewing official has disqualifying information regarding an individual, the reviewing official should make the access determination. Therefore, the Commission has revised the proposed rule text in the final rule to reduce unnecessary regulatory burden by providing licensees and applicants the flexibility to terminate the process upon receipt of disqualifying information. To increase the clarity in the organizational structure of the requirements set forth in paragraph (h), the Commission moved paragraphs (h)(1), (h)(2), (h)(8), (h)(9), and (h)(10) to paragraphs h(5), h(6), (h)(1), (h)(2), and h(3), respectively, in the final rule.

Comment Summary:
One commenter, supported by many other commenters, stated that this provision requires licensees to grant access to individuals certified by the NRC but does not provide details about certification nor state that the certification process shall be consistent regardless of which NRC office or region provides it. The commenter recommended that the final rule should require a consistent certification process, with the certifications originating from a small group within the NRC identified beforehand to licensees.

NRC Response:
The NRC disagrees with the comment because the certification requirements set forth in the proposed 10 CFR 73.56(h)(9) are consistent with long-standing NRC- practice. 10 CFR 73.56(c)(3), in the former rule, required licensees to grant unescorted access to individuals who have been certified by the NRC as suitable for such access. To assist licensees in meeting this requirement, each Regional Office has a Division of Resource Management and Administration (DRMA) and has developed a procedure and a licensee site visit notification letter to notify nuclear power plant sites of visits by NRC employees and NRC contractors. The site visit

notification letter contains a visiting individual's name, badge number, and clearance. The need for site specific training is usually determined by the licensee when the NRC employees and NRC contractors first arrive at a site. Thus, any licensee who has concerns or questions regarding NRC employees' or contractors' site visits can easily and promptly have the issues addressed or questions answered by contacting their Regional DRMA representative.

Comment Summary:
Two commenters jointly stated that proposed 10 CFR 73.56(h)(10) would allow individuals known to be escaped felons or on the terrorist list to be escorted into protected and vital areas. The commenters said that the intention to prevent individuals who have formally been denied unescorted access to a nuclear power plant from entering a nuclear power plant as a visitor is commendable, but this provision was too narrowly defined. The commenters noted that there have been cases, as the NRC is aware, where licensees have come across derogatory information during background checks that would have resulted in unescorted access being formally denied, but stopped the process at that point and simply escorted the individuals into the protected area anyway.

The commenters recommended that the NRC regulations must prevent licensees possessing derogatory information about individuals that would prevent them from being granted unescorted access from allowing said persons inside the protected area fence even as escorted visitors.

NRC Response:
The Commission disagrees with the comment. The Commission finds that the proposed regulations include the following provisions to address the commenter's security concerns regarding a licensee allowing an individual to be escorted in its nuclear power plant protected area after a licensee has discovered derogatory information about the individual while processing the individual's unescorted access application:

1. 10 CFR 73.56(d)(1)(ii) requires licensees to complete background investigation elements once they are initiated and to record the findings and the individual's access authorization status. The collected information (such as derogatory information) is shared with other licensees.

2. 10 CFR 73.56(h)(1) requires licensees to evaluate all the information specified in 10 CFR 73.56 before its reviewing official determines whether an individual is trustworthy and reliable. However, it allows licensees to deny anyone as soon as it obtains disqualifying information about an individual.

Therefore, the Commission finds that the rule is adequate in addressing this comment. Finally, the Commission finds that the comment regarding allowing individuals known to be escaped felons or on the terrorist list to be escorted into protected and vital areas of nuclear power plants, is beyond the scope of this section. This section specifically provides regulations regarding individual's unescorted access and unescorted access authorization. The NRC regulations regarding escorted access are sufficiently addressed in 10 CFR 73.55.

Comment Summary:
One commenter, supported by many other commenters, stated that the provision requires licensees and applicants to develop reinstatement review procedures for assessing individuals who have been in an access denied status, but power reactor licensee procedures already

require such an assessment. Thus, the commenter recommended that the Commission revise 10 CFR 73.56(h)(10) to state: "Licensees and applicants may not permit an individual, who is identified as having an access-denied status in the information-sharing mechanism required under paragraph (o)(6) of this section, or has an access authorization status other than favorably terminated, to enter any nuclear power plant protected area or vital area, under escort or otherwise, or take actions by electronic means that could impact the licensee's operational safety, security, or emergency response capabilities, under supervision or otherwise, except upon completion of the initial unescorted access authorization process, if the Reviewing Official determines that such access is warranted".

NRC Response:
The Commission agrees that the regulation that requires licensees and applicants to develop reinstatement review procedures for assessing individuals who have been in an access denied status is unnecessary, because paragraph (h)(3) provides requirements regarding such individuals. Therefore, the Commission deleted this requirement from the final rule.

Comment Summary:
One commenter, supported by many other commenters, stated that 10 CFR 73.56(i)(1)(iv) incorrectly indicated that a licensee's Physical Security Plan contains details about the Behavioral Observation Program (BOP). In fact, BOP documents, not the Physical Security Plan, contain these details. Therefore, the commenter recommended that 10 CFR 73.56(i)(1)(iv) be revised by substituting "Behavior Observation Program" for "Physical Security Plan" as the source of BOP details.

The commenter also noted that this section required that individuals be subject to a "supervisory interview" rather than to a "supervisory review." The commenter said that this wording was inconsistent with the industry's practice of basing the annual supervisory review on the year's interactions between the supervisor and the individual, not on just a single interview. Because the industry believes that the Commission intended that it continue with this effective current practice, the commenter recommended that the section be revised by indicating that the individual is to be subject to a "supervisory review" rather than to a "supervisory interview."

Lastly, the commenter stated that the word used in NRC-approved industry documents regarding the frequency of the review is "annual" rather than "nominal 12-month." Therefore, he recommended that 10 CFR 73.56(i)(1)(iv) be revised to substitute "annual" for "nominal 12-month".

NRC Response:
The Commission agrees with the comments regarding the incorrect characterization of the Physical Security Plans and the details of the BOP. The Commission finds that details of behavior observation are described in the access authorization program instead of plants' Physical Security Plan. Therefore, the Commission revised the final rule text to correct this error.

With regard to the comment concerning used of the term "nominal 12-month" rather than "annual," The Commission agrees in part with this comment. The intent of this requirement is that the supervisory review/interview be conducted on a nominal annual basis for each individual with unescorted access authorization or unescorted access maintained for 365 consecutive days. The periodicity of the annual supervisory interviews/reviews is consistent with the current industry practice.

Finally, with regard to the recommendation to replace the term “interview” with “review,” the Commission agrees in part with the comment. Specifically, the Commission disagrees that 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 and close observation by supervisors less common and difficult to achieve. The Commission recognizes that there are many instances in which supervisors will have sufficient information about an individual through frequent observations and interactions with their employees over the course of the review period. Therefore, the NRC revised the final rule to address both the instances where supervisors have and do not have sufficient information about an individual over the course of the review period.

Comment Summary:
One commenter, supported by many other commenters, noted that that requiring a psychological reassessment of individuals within five years of the date on which such an assessment was last completed goes beyond the requirements of the Access Authorization Order, dated January 7, 2003. The commenter stated that requiring five-year psychological reassessments will have significant cost and negligible benefit. The commenter argued that, since all other aspects of the access authorization requirements are repeated at the five-year interval already, and the BOP is continuous, this obviates the need for such a reassessment for an individual maintaining access.

Another commenter noted that the Commission has concluded repeatedly that the current requirements provide high assurance of mitigation for various aspects of the insider threat and has not provided justification for this new requirement. Yet another commenter added that in the statement of considerations the Commission noted that this proposed requirement provides consistency with other entities that need trustworthy and reliable employees but does not specify with which entities consistency will be achieved. This commenter stated that no other justification or benefit of the new and burdensome requirement was discussed in the Federal Register Notice or in the Draft Regulatory Analysis. Thus, with no obvious benefit for a very costly requirement, the commenters strongly recommended that the Commission delete the proposed requirement from the final rule.

NRC Response:
The Commission agrees, in part, regarding the proposed 5-year psychological reassessments. The Commission agrees that requiring psychological evaluation as part of the 5-year review for all individuals maintaining unescorted access or unescorted access authorization status will add significant costs and deviates from the intent of the current requirements. Therefore, to minimize the unnecessary regulatory burden on licensees and to maintain the intent of the previous regulations, the Commission has revised the final rule text to limit the group of individuals who are subjected to 5-year psychological reassessments to those individuals who perform job functions that are similar to the group of individuals who are currently identified as warranting psychological assessment every 5 years. Specifically, the groups of individuals that require 5 -year psychological reassessments are those individuals who have one or more following job functions:

Any individual who has extensive knowledge of defensive strategies and design and/or implementation of the plant’s defense strategies, including
- Site security supervisors
- Site security managers

- Security training instructors
- Corporate security managers

Any individual in a position to grant an applicant unescorted access or unescorted access authorization, including
- Site access authorization managers

Any individual assigned a duty to search for contraband (i.e., weapons, explosives, incendiary devices)

Any individuals who secures plant networks or security system networks, or have extensive knowledge of plant networks, or have administrative control over the plant networks, including
- Plant network systems administrators
- IT personnel who are responsible for securing plant networks.

Any individual qualified for and assigned duties as: armed security officers, armed responders, alarm station operators, and response team leaders as defined in the licensee'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. Non-licensed operators also monitor plant instrumentation and equipment and principally perform their duties outside of the control room.

The Commission disagrees with the assertion that the BOP obviates the need for a psychological reassessment. The BOP provides a way to detect an individual's emotional and/or psychological state at a given point in time. It is not designed to identify changes in individuals' overall psychological well-being. Thus, the Commission finds that that a psychological reassessment is warranted for those individuals who perform job functions that pose a threat similar to those job functions that are currently required to be psychologically assessed every 5 years.

Finally, the Commission has revised the phrase "every 5 years of the date on which these elements were last completed, or more frequently," to identify and specify those individuals who are required for criminal history and credit history reevaluation every 3 years to maintain his or her unescorted access or unescorted access authorization.

Comment Summary:
One commenter, supported by many other commenters, stated that 10 CFR 73.56(i)(1)(v)(B) assumed that the industry conducts the processes used to assure that an individual continues to be trustworthy and reliable concurrently when, in fact, it does not. The commenter noted that the criminal history update and credit history re-evaluation (reinvestigation) are normally conducted concurrently. However, proposed 10 CFR 73.56(i)(1)(v)(A) required that these processes be conducted within 5 years of the date on which these elements were last completed.

Since there is no requirement for all these elements to be initially completed at the exact same time, the commenter thought that imposition of a requirement for completion of a five-year update within 30 days of initiating any of the elements would require updating of some of these elements at intervals of less than five years. The commenter said that the frequency of the annual supervisor review was addressed in the proposed 10 CFR 73.56(i)(1)(iv) and did not

need to be included in proposed 10 CFR 73.56(i)(1)(v)(B).

As noted above, the commenter said that the industry recommends the psychological reassessment not be required. Finally, the commenter recommended that there should be no requirement regarding the length of time spent on the required elements. Instead, this section should require that the elements should be completed approximately concurrently. For these reasons, the commenter recommended that 10 CFR 73.56(i)(1)(v)(B) be revised by deleting the mention of the annual supervisor review and the psychological reassessment and by allowing the reviewing official to complete the evaluation of the information obtained from the criminal history update and credit history reevaluation "within 30 calendar days of completing the review of the other of these elements" rather than "within 30 calendar days of initiating any one of these elements".

NRC Response:
The NRC agrees with the received comment. Therefore, the NRC has revised the proposed rule text in the final rule to state that only the criminal history update and the credit history re-evaluation shall be completed within 30 calendar days of each other.

Comment Summary:
One commenter, supported by many other commenters, thought that the mention in proposed 10 CFR 73.56(k)(1)(ii) that a local criminal history review and evaluation from the State of the individual's permanent residence" was not clear. Based on the proposed rule's Statement of Considerations, the commenter stated that the industry believes that the NRC intends that licensees obtain a criminal history from the police agency serving the individual's permanent residence. The commenter noted, however, that industry experience is that the court system, with its public records, can be a better source of criminal history information than local law enforcement agencies. Also, local law enforcement agencies may not have the staff or budget to provide criminal history information. The commenter recommended that the rule should provide flexibility to pursue the best source of information. The commenter suggested that the Commission revise 10 CFR 73.56(k)(1)(ii) to specify a local criminal history review and evaluation from the court or police agency serving the individual's permanent residence.

NRC Response:
The Commission agrees with the commenter's recommendation on the need for flexibility in pursuing to obtain the best information concerning local criminal history information. Thus, the Commission has revised the final rule text to reflect this comment.

Comment Summary:
One commenter, supported by many other commenters, stated that the final rule should permit the flexibility to use, in lieu of a local criminal history review and evaluation from the State of the individual's permanent residence, the criminal history check required by the proposed 10 CFR 73.56(d)(7). That section provided that the reviewing official shall evaluate the entire criminal history record of an individual applying for unescorted access authorization and that the criminal history record must be obtained in accordance with the requirements of 10 CFR 73.57.

NRC Response:
The Commission agrees with the recommendation to allow licensees to use the criminal history check required by proposed 10 CFR 73.56(d)(7) in lieu of a local criminal history review. The Commission revised the final rule text to allow the use of either criminal history check.

Comment Summary:
One commenter, supported by many other commenters, noted that 10 CFR 73.56(m)(1) would require licensees, applicants, and contractors/vendors to disclose employee personal information to NRC representatives. The commenter said that the industry believes that a very limited number of NRC representatives require access to the personal information of employees and recommended that 10 CFR 73.56(m)(1) be revised to provide that industry employee personal information should be accessible only to NRC resident inspectors and NRC inspectors performing inspections for compliance with 10 CFR 73.56. The commenter said that such limited access to this information would be consistent with the requirements for protection of personal information in the Access Authorization Order, dated January 7, 2003.

NRC Response:
The Commission disagrees with the comment that industry employee personal information should be accessible only to NRC resident inspectors and NRC inspectors performing inspections. Although the Commission agrees that personal information should only be disclosed to NRC representatives who have a legitimate reason to obtain the information, the NRC extends this legitimate need beyond NRC inspectors, such as the NRC obtaining this personal information for Terrorist Screening Center (TSC) checks.

The Commission's position is that listing specific NRC representatives in the rule could create the potential that requests by NRC representatives who have a legitimate need to obtain this information could be refused, resulting in protracted action to obtain the information that would not be in the best interest of protecting the public health and safety and common defense and security. In addition, the Commission is not aware of any instances in which NRC representatives without a legitimate need have attempted to obtain this kind of personal information. For these reasons, the NRC has retained the wording as proposed.

Comment Summary:
One commenter, supported by many other commenters, noted that 10 CFR 73.56(m)(3) required licensees to provide copies of all records pertaining to a denial or unfavorable termination of the individual's unescorted access authorization to designated representatives of the individual but did not describe a means for the licensee to verify that the representative is legitimate. The commenter noted that 10 CFR 73.56(m)(1)(i) required the individual to designate the representative in writing, and that 10 CFR 73.56(m)(3) should be revised to also require the individual to designate the representative in writing. Additionally, the commenter argued that licensees should be required to provide only the information pertinent to the denial or unfavorable termination, not the entire record.

Finally, the commenter noted that 10 CFR 73.56(m)(3) did not permit licensees, applicants, and contractors or vendors to exclude identification of the sources of the information provided, as is permitted currently. The commenter stated that this exclusion is important to ensure that sources who provide such information will continue to do so.

NRC Response:
The Commission agrees with the comments and revised paragraph (m)(2) of the final rule to specify that representatives must be authorized by the individual in writing and that information pertaining to the source may be redacted to protect the source. The Commission agrees with the comments because these requirements are necessary to ensure the protection of personal information.

Comment Summary:
One commenter, supported by many other commenters, noted that 10 CFR 73.56(n)(1) would require licensees to perform audits of access authorization programs at a frequency of no less than nominally every 24 months. The commenter argued that the NRC discussion of the proposed rule indicated that audits accomplish their objectives at the current 24-month frequency and that there was no discussion regarding any benefit of a shorter frequency or discussion of the complexity of arranging audits at irregular intervals. The commenter argued that, for a program performing well enough to merit auditing at the maximum frequency, a 25 percent margin should be provided. Thus, the commenter recommended that the Commission revise 10 CFR 73.56(n)(1) to state: "Each licensee, applicant and C/V [contractor/vendor] who is subject to this section shall ensure that the full scope of their authorization program is audited as needed, but no less frequently than nominally every 30 months."

NRC Response:
The NRC disagrees with the received comment because the definition of "nominal" in 10 CFR Part 26 includes a 25 percent margin. Therefore, the required 24-month nominal auditing frequency would extend the auditing frequency up to 30 months.

Comment Summary:
One commenter, supported by many other commenters, said industry believed that the Commission intended in 10 CFR 73.56(n)(4) to provide that auditors be granted access to any documents needed and that auditors should be able to take away copies of documents rather than the original documents. Therefore, the commenter recommended that "copies of any documents and take away any documents" be replaced with "any documents and to take away copies of any documents".

NRC Response:
The Commission agrees that the rule should require access to any documents needed and to allow copies rather than original documents to be taken away and has revised the text in the final rule to incorporate this recommendation.

Comment Summary:
One commenter, supported by many other commenters, thought that 10 CFR 73.56(n)(5) did not account for the fact that contractor/vendor programs are audited. The commenter argued that it is not reasonable to require the audit team for contractor/vendor audits to include a person who is knowledgeable of and practiced with meeting authorization program performance objectives and requirements. Instead the commenter said the contractor/vendor audit team should include a person who is knowledgeable of and practiced with meeting authorization program performance objectives pertinent to the contractor/vendor's scope of work.

Additionally, the commenter noted that many contractor/vendors do not have people who are independent from both the subject authorization program's management and from personnel who are directly responsible for implementing the authorization program(s) being audited. Therefore, the commenter recommended that 10 CFR 73.56(n)(5) be revised in the following ways: 1) the requirement for inclusion of "a person who is knowledgeable of and practiced with meeting authorization program performance objectives and requirements" should be applied to teams auditing licensee and applicant, but not contractor/vendor, authorization programs; 2) the requirement that individuals performing an audit "shall be independent from both the subject authorization program's management and from personnel who are directly responsible for

implementing the authorization program(s) being audited“ should be applied to teams auditing licensee and applicant, but not contractor/vendor, authorization programs, and 3) at least one member of a team auditing a contractor/vendor program should be “a person who is knowledgeable of and practiced with meeting the authorization program performance objectives and requirements within the scope of work the contractor/vendor performs”.

NRC Response:
The Commission disagrees with the comment that requests the final rule to include specific audit requirements for contractors or vendors. This requirement applies to licensees and applicants who are responsible for meeting the requirements of this section. The intent of this requirement is for licensees and applicants to perform audits of their access authorization program to include those program elements that are provided by contractors and vendors.

Comment Summary:
One commenter, supported by many other commenters, argued that the 10 CFR 73.56(n)(6) requirement for licensee distribution of audit reports should be consistent with 10 CFR 50 Appendix B, Section XVIII., “Audits.” The commenter claimed that doing otherwise would create an impossible situation because the Audit Program is configured to conform to Appendix B requirements. To accomplish this consistency, the commenter recommended that 10 CFR 73.56(n)(6) be revised to provide that audit results must be reported to “management having responsibility in the area audited” rather than to “senior corporate and site management”.

NRC Response:
The Commission agrees with the commenters that paragraph (n)(6) should be consistent with 10 CFR 50, Appendix B. Additionally, the Commission finds that audit reports should be provided to a management at a high enough level to ensure proper disposition and oversight of issues identified during the conduct of audits. Therefore, the Commission has revised the final rule paragraph (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.

Comment Summary:
One commenter, supported by many other commenters, noted that 10 CFR 73.56(a)(6) provided that only licensees and applicants, but not contractor/vendors, can grant or permit an individual to maintain unescorted access to nuclear power plant protected areas. Therefore, only licensees and applicants would have records pertaining to denial or unfavorable termination of unescorted access authorization and related management actions. For this reason, the commenter recommended that the Commission remove the reference to contractor/vendors in 10 CFR 73.56(o)(2), making its record retention requirements applicable to licensees and applicants but not to contractor/vendors.

The commenter also noted that 10 CFR 73.56(h)(10) provided that there is no time limit on the prohibition for an individual, who is identified as having an access-denied status in the information-sharing mechanism, from gaining access to the protected area of a nuclear power plant. Therefore, the commenter recommended that 10 CFR 73.56(o)(2) provide that the records pertaining to denial or unfavorable termination of unescorted access authorization and related management actions must be maintained as long as the licensee or applicant is an NRC licensee or applicant.

NRC Response:
The Commission agrees with the commentes regarding maintaining records pertaining to denial or unfavorable termination of unescorted access or unescorted access authorization and related management actions as long as the licensee or applicant is an NRC licensee or applicant. Therefore, the Commission revised the final rule text to reflect this comment.

Additionally, although the Commission agrees that only licensees and applicants can grant, certify, permit an individual to maintain, withdraw, deny, or terminate unescorted access or unescorted access authorization status, the Commission disagrees with the assertion that contractors or vendors do not have records that are pertinent to granting, denying, or terminating unescorted access authorization. In fact, contractors or vendors often develop information that is used in access authorization determinations including maintaining individuals' access authorization. For example, a contractor or vendor may provide behavioral observation training and maintain the records.

Therefore, the Commission added the last two sentences to the final rule text to allow contractors or vendors to maintain those records that they collected for applicants and/or licensees as long as they meet the requirements set forth in 10 CFR 73.56. Also, in consideration of the commenters recommendations, the Commission has revised the proposed rule to require that contractors and vendors provide to licensees and applicants all records that have been collected on behalf of the respective licensee or applicant, upon termination of any contract between the licensee or applicant and the contractor approved program.

Comment Summary:
One commenter, supported by many other commenters, noted that 10 CFR 73.56(o)(6) indicated that the information-sharing mechanism is established and administered by licensees, applicants, and contractor/vendors, but the information-sharing mechanism currently exists and was established by licensees only. The commenter argued that the industry believes that only those who can grant or maintain access, i.e., licensees and applicants, should administer the information-sharing mechanism. The commenter noted that the industry group that oversees the information-sharing mechanism does include three contractor/vendor representatives and industry intends to maintain this representation indefinitely.

Additionally, the commenter recommended that 10 CFR 73.56(o)(6) be revised to state that "all users" of the information sharing mechanism, rather than "licensees, applicants, and contractor/vendors," have responsibility for ensuring that only correct information is put into the mechanism. Also, the commenter noted that the information-sharing mechanism does not contain records; it contains data representative of the records. Further, the commenter noted that the Access Program is typically described in the Access Program Procedure rather than the Physical Security Plan.

Lastly, the commenter stated that 10 CFR 73.56(o)(6) indicated that records in the information-sharing mechanism must be available for NRC review. The commenter said that access to the information-sharing mechanism is available at licensee power reactor sites or at the central location for the information-sharing mechanism. The commenter argued that licensee power reactor sites are available to NRC inspectors continually, however, it is not practical to maintain continuous access at the information-sharing mechanism central location. Thus, the commenter recommended that the Commission revise 10 CFR 73.56(o)(6) in the final rule to state that data maintained in the database must be available for NRC review with reasonable notice."

NRC Response:
The Commission agrees that the information-sharing mechanism does not contain records. It contains data representative of the records. The Commission revised the final rule text to correct this error. Additionally, the NRC agrees with commenters regarding who can access information-sharing mechanism. However, the Commission did not use the term “user” recommended by the commenter. Instead, the NRC revised the proposed rule to state “licensee, applicant, or the contractor or vendor who have been authorized to add or manipulate data in an information sharing mechanism” for clarity.

Finally, the Commission agrees with the recommended change regarding data maintained in the database available for NRC review. However, the Commission did not use the term “with reasonable notice.” Instead, the Commission used term “as soon as reasonably possible.” The information sharing mechanism is a licensee administered vehicle for the express purpose of managing information that allows licensees, applicants to take credit for the access authorization program actions, which comply with the requirements set forth in this section, taken by other licensee, applicants or contractor or vendors. Therefore, the NRC must be able to access the information sharing mechanism as soon as reasonably possible, for the purpose of conducting inspections or investigations, performing audits or generally ensuring that regulatory requirements are being met.

10 CFR 73.58 Safety/Security Interface Requirements for Nuclear Power Reactors Responses to Public Comments

Comment Summary:
Commenters indicated that the proposed rule language adds several programmatic requirements for security that are currently managed through other site programs such as configuration control programs, risk assessment programs, the technical specifications, and work management processes. The commenters stated that imposing the assessment and management of physical modifications, system reconfiguration, maintenance activities, emergent activities, and other departmental responsibilities onto security would significantly impact and detract from security's primary mission of securing and protecting the plant. Thus, the commenters stated that the NRC should revise the proposed rule to take credit for all the existing management programs that are in place and only impose changes related to the security plan and implementing procedures in a security regulation.

NRC Response:
The NRC agrees in part. It is not the intent of this new requirement to impose new broad programmatic requirements on licensees. If current programs and procedures are in place to enable the safety/security interface to be assessed and managed, then those procedures and programs should be used.

The NRC recognizes that increased complexity would only detract from the objectives of this new requirement (to ensure that neither safety nor security is compromised due to the other's activities). The NRC wants licensees to rely upon, and take credit for, currently existing processes to the maximum extent practical. If current work management processes and configuration control programs are adequately controlling facility activities to preclude adverse interactions between safety and security, then these processes should be utilized.

However, it may be necessary for these processes to be revised to account for (if they do not currently) the potential for adverse safety and security interactions. In other cases, the current processes already account for these adverse interactions. Changes to these processes may be made to simply raise the awareness of potential interactions, particularly for areas of the facility where traditionally such interactions would not occur (from a power operations/safety standpoint, there exists a potential to adversely impact security (e.g., in the owner controlled area)). In fact, changes to currently existing processes may be the most efficient means to preclude adverse interactions for normal, day-to-day activities.

The NRC recognizes that various plant programs address the safety/security interface issue to some extent, such as, design change control, procedure change control, and maintenance order review processes. It is the NRC's view, that given the large effort that has been focused onto the processes that control planned changes to the facility (i.e., 10 CFR 50.59 requirements and the supporting guidance) in recent years, that the 10 CFR 73.58 requirements will primarily impact the security-side of the facility (i.e., assessing facility activities to determine whether some aspect of facility security is impacted).

In this regard, the NRC believes that it is important that security expertise be involved in the assessment and management of facility changes since it is not obvious in some cases where activities that may not be important for safety can impact facility security. But the NRC does not envision a large, cumbersome (and impractical) program to assess all ongoing activities. The commenter suggests that the NRC should revise the proposed rule to take credit for existing

programs. The NRC does not believe this type of modification (to rule language) is necessary and that this level of detail, which involves the means by which licensees might comply with the rule requirements, can be best addressed in the guidance that NRC will issue to support 10 CFR 73.58. In summary, the NRC does not intend to impose new broad programmatic requirements in this section and, instead, expects that licensees would make maximal use of existing programs.

Comment Summary:
The commenter stated that this section provides general guidance that, if interpreted broadly, could require an explicit review for any change (e.g., editorial changes to procedures may require an explicit assessment). The commenter suggested that NRC consider instituting a screening process.

NRC Response:
The NRC agrees with the commenter that implementing 10 CFR 73.58 in such a fashion would be unduly burdensome, and counter-productive. It is the intent of this requirement that changes to the facility that can adversely impact safety or security be assessed and managed. The NRC recognizes that many changes can not have such an impact, and these changes can be readily screened out. Also, the NRC expects that many other changes would be controlled through work control type processes (where adverse interactions are precluded) and, in such situations, the process itself is managing the safety and security interface. The NRC believes that this type of issue is best dealt with in the supporting guidance to 73.58, and did not revise the final rule language.

Comment Summary:
The commenter stated that the SOCs cite "variables in the current threat environment" as one justification for the new requirement. The commenter asked: "Does that mean a threat greater than the DBT?"

NRC Response:
The safety security requirements are being imposed on licensees as cost-justified safety enhancements per the criteria in 10 CFR 50.109. It is the Commission's view that 10 CFR 73.58 will enhance the management and assessment process at facilities and preclude/reduce adverse interactions, and that the costs are justified in view of these enhancements per 10 CFR 50.109(a)(3).

The statement citing variables in the current threat environment is misleading, and can be interpreted to mean that 10 CFR 73.58 is required to ensure adequate protection of public health and safety to defend against the revised post September 11, 2001 design basis threat, which is not the case. The final rule language has been revised to remove the statement in question, as well as other similar verbage that can be misinterpreted by stakeholders to cause them to conclude that this new requirement is necessary for adequate protection of public health and safety.

Comment Summary:
The commenter stated that the SOCs reference plant events that demonstrate that changes to the facility, its security plan, or implementation of the plan can have adverse effects. The commenter stated that it would be beneficial if the NRC shared these events with industry so they can be captured in lessons learned.

NRC Response:
The NRC agrees. In fact, the NRC issued Information Notice 2005-33 "Managing the Safety/Security Interface" where this information was shared with industry. The SOCs supporting 10 CFR 73.58 have been revised to reference this information notice.

Comment Summary:
The commenter asked, "If a licensee is implementing a measure to comply with a regulation, does this provision apply?" The commenter stated that the rulemaking process should require the Commission to conduct a safety/security interface assessment before any rule is promulgated.

NRC Response:
Measures used to implement Commission requirements are subject to safety/security interface. As a general rule, licensees are required to comply with the regulations, and through such compliance ensure that the activities at the facility provide reasonable assurance of public health and safety and common defense and security. Prior to issuance of 10 CFR 73.58, licensees were required to ensure that facility activities did not adversely impact safety or security (otherwise the activity would have caused the license to fail to comply with the governing requirements in the respective area). Section 73.58 makes explicit what was already an implicit requirement, and thus is considered by the NRC to be a more coherent regulation. The SOCs supporting 10 CFR 73.58 were revised to reflect this fact.

Regarding the other aspect of this comment, the NRC is not a licensee nor applicant, and as such, is not subject to the requirements of 10 CFR 73.58. However, the NRC is sensitive to the potential adverse impacts of new regulations, and when such impacts are known, the NRC attempts to factor them into its regulatory analysis supporting the new requirements.

Comment Summary:
The commenter stated that this new requirement is lacking in a performance standard.

NRC Response:
The NRC disagrees. The performance-standard for 10 CFR 73.58 is clearly stated in paragraph (b). The rule states that, "Where potential adverse interactions 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."

The NRC believes that this is a reasonably clear performance standard. The NRC did not elect to be more prescriptive with the standard in the rule since such prescription is generally counter to good regulation, and additionally such prescription may become too limiting to address the wide variety of situations that might occur. Instead, the NRC elected to support this requirement with guidance that would assist licensees in determining how best to comply with the standard. No changes to the final rule or supporting SOCs were made as a result of this comment.

Comment Summary:
Another commenter stated that this provision satisfies the Union of Concerned Scientists' (UCS's) concerns that prompted UCS to petition the NRC. The commenter noted that during the NRC public meeting on March 9, 2007, an industry working group representative asserted that this requirement was too onerous, too burdensome, and too complex for his company to implement. The commenter argued that a competent licensee should have no difficulty meeting

this requirement with little burden.

NRC Response:
The NRC agrees. The NRC agrees that the requirements of this section address a portion of Petition for Rulemaking (PRM) 50-80. The NRC also believes that the concerns raised by industry are a result of an interpretation of 10 CFR 73.58 that assumes that it is imposing new, broad programmatic requirements onto the licensee. This is not the intent as has been discussed in previous comment responses. No revisions were made to the final rule or SOCs as a result of this comment, although the SOCs were revised to reflect the fact that NRC does not intend to impose new broad programmatic requirements in this section.

Comment Summary:
A commenter, following a lengthy discussion of proposed 10 CFR 73.58, recommended that the NRC consider pursuing enhancements to the existing processes or at least ensure that the final rule acknowledges the acceptability of the regulations already in place.

NRC Response:
The NRC agrees. The intent of this requirement is to ensure the each licensee evaluates and utilizes the information currently available from existing programs and ensures the effective interface between these existing programs in a manner that ensures the public health and safety. As mentioned in response to two previous comments, the SOCs were revised to reflect the fact that the NRC does not intend to impose broad, new programmatic requirements by this section, and that the NRC expects licensees to make maximal use of current programs. It is probable that this language would result in enhancements to current procedures and processes to make more explicit reference to 10 CFR 73.58.

Comment Summary:
One commenter stated that the title should indicate that the training is for security personnel. Thus, the commenter recommended that the Commission change the title in the final rule to "Nuclear Power Reactor Security Personnel Training and Qualification Plan."

NRC Response:
The Commission agrees in part. The Commission agrees that this title should be revised to clarify applicability. However, the Commission disagrees with the suggested change. This title is revised to clearly identify that this training and qualification (T&Q) plan addresses T&Q for security program duties being performed and is not limited by position or organization titles within the security organization. The T&Q requirements of this Appendix also apply to non-security organization personnel performing security duties.

Comment Summary:
Another commenter supported the detailed NEI comments for Appendix B and stated that it has incorporated much of the detailed guidance of NEI 03-09 as regulatory requirements. The commenter noted that this detail is more appropriate as guidance versus requirements, and inclusion in a rule undermines standardization by reintroducing site specific detail that is better contained in implementing procedures alone.

NRC Response:
The Commission disagrees. The licensee may implement Commission requirements through the T&Q plan and implementing procedures. The requirements of this Appendix have been updated to provide the regulatory framework for the plans and procedures referred to by this comment. One of the primary purposes of this rulemaking is to update the regulatory framework to more accurately represent the requirements for NRC-licensed facilities. Therefore, the Commission disagrees that the updated rule text in this Appendix is better contained in implementing procedures, but rather believes that these requirements are implemented through the implementing procedures referred to by this comment.

Comment Summary:
One commenter stated that proposed Part 73, Appendix B, A.1 and associated SOCs imply that "any individual who is assigned to perform a security function" is now expected to "meet minimum training and qualification requirements." The commenter stated that this could be very broadly interpreted to apply to many and varied licensee positions, including access authorization, FFD, computer technicians, contractors, plant operators, etc. The commenter said that additional definition or clarification may help minimize regulatory interpretation. The commenter stated that this consideration is more expansive, either by mistake or intent, than A.3, which clearly limits some requirements to the "security organization." The commenter recommended that the Commission revise this provision in the final rule by replacing "all individuals" with "all security personnel."

NRC Response:
The Commission agrees in part. The Commission explicitly intends to require that "any individual who is assigned to perform a security function" is now expected to "meet minimum training and qualification requirements" for those assigned duties whether the individual is a

member of the security organization or other facility staff. Any person assigned to perform a physical protection and/or contingency response duty must be trained & qualified to ensure they can physically and mentally perform the assigned duty. In specific areas of this appendix where the applicability is limited to security personnel, the requirement clearly identifies this limited applicability. The Commission disagrees that Paragraph A.3 is limited to only security organization personnel. Therefore, the Commission disagrees with the suggested rule text change and has retained the phrase "all individuals" as this is the intent of this generic requirement.

Comment Summary:
The same commenter noted that proposed 10 CFR 73, Appendix B, A.1 SOCs state that implementation of the Commission-approved security plans, licensee response strategy, and implementing procedures would provide a detailed list of programmatic areas for which the licensee must provide effective T&Q to satisfy the performance objective for protection against radiological sabotage. The commenter stated that "detailed list of programmatic areas" is undefined and asked if this is the listing of Critical Tasks or the Task List proposed by NEI. The commenter recommended that the Commission clarify the proposed Part 73 Appendix B, A.1 SOC to state:

> "The programmatic areas are listed in the Commission approved Training and Qualification plan for each licensee. Specific training and qualification requirements to support these areas are derived by the licensee during the use of the graded Systematic Approach to Training process. Training elements and Qualification criteria are specific to each licensee."

NRC Response:
The Commission disagrees with the suggested SOC text change because the Commission does not intend to require a graded systematic approach to training for each licensee. The Commission agrees that the detailed list of programmatic areas is undefined because that list is unique and different at each site and can only be addressed generically in this rule. Therefore, each site is responsible to document this list as part of the T&Q plan whether they choose a systematic approach to training or another acceptable method for their training process.

Comment Summary:
One commenter stated that the proposed Part 73, Appendix B, A.2 and SOCs do not, but should, recognize the Systematic Approach to Training process. The commenter recommended that the Commission revise proposed Part 73, Appendix B, A.2 in the final rule by adding the following sentence to the end of the provision:

> "The minimum training and qualification areas are listed in the Commission-approved Training and Qualification plan for each licensee. Training and qualification requirements to support these areas are derived by the licensee during the use of the graded Systematic Approach to Training process. Training elements and qualification criteria are specific to each Licensee."

NRC Response:
The Commission disagrees with the suggested rule text change because the Commission does not intend to require a systematic approach to training for each licensee. The Commission agrees that the detailed list of programmatic areas is undefined because that list is unique and different at each site and can only be addressed generically in this rule. Therefore, each site is

responsible to document this list as part of the T&Q plan whether they choose a systematic approach to training or another acceptable method for their training process.

Comment Summary:
One commenter stated that the requirement to "simulate" was not previously in Part 73. The commenter stated that this term carries a different meaning than "consider."

NRC Response:
The Commission agrees that the stated requirement to simulate was not previously contained in Part 73. The intent is to "simulate" and not simply consider. The Commission's expectation is that personnel shall be trained in a manner which simulates the site specific conditions under which the assigned duties and responsibilities are required to be performed.

Comment Summary:
Another commenter stated that proposed 10 CFR 73, Appendix B, A.7 does not recognize the changes proposed in Security Frequently Asked Questions (SFAQ) 05-17, "Scheduling of Annual Training." The commenter noted that this SFAQ describes a proposed change to NEI 03-09, "Security Officer Training Program," Section 8.2, "Training Periodicity," as follows: "The licensee may schedule training at an earlier date which may then be used as the basis for scheduling the next training requirement. This 'short-cycled' training will always result in more training than the minimum required by requirements. This new scheduled date is the basis for the next scheduled date." Thus, the commenter recommended that the Commission revise Part 73, Appendix B, A.7 in the final rule by adding the following sentence to the end of the provision:

> "The licensee may schedule training at an earlier date which may then be used as the basis for scheduling the next training requirement. This 'short-cycled' training will always result in more training than the minimum required by the Commission-approved Training and Qualification plan. This new scheduled date shall be the basis for the next scheduled date."

NRC Response:
The Commission disagrees with adding SFAQ 05-17 "scheduling of Annual Training" to the rule text. SFAQ 05-17 is a draft document and not a final NRC position. The draft SFAQ will be incorporated into the regulatory guide for training and qualification and will provide guidance on this issue. The intent of this requirement is to provide the licensee with the necessary flexibility to resolve scheduling issues due to unexpected circumstances.

Comment Summary:
One commenter stated that proposed 10 CFR 73, Appendix B, B.1.b and associated SOCs add the phrase "by a qualified training instructor." The commenter stated that this blanket addition located throughout the proposed changes to Appendix B will create a huge administrative burden and add additional cost as processes overseen by other organizations (such as Medical) will now require administration by a qualified training instructor.

The commenter noted that there is no definition of "qualified training instructor," which will lead to confusion regarding compliance. The commenter noted that the current basis for the change does not identify a performance or regulatory gap, and the proposed change creates a regulatory gap where none existed before. Thus, the commenter recommended that the Commission restore the proposed wording to that in the existing Appendix B to state: "The qualifications of each individual must be documented and attested by a licensee security

supervisor."

NRC Response:
The Commission disagrees and has retained the proposed language as written. The Commission has determined that currently, many licensees employ training instructors to manage and direct the oversight of their security training program. This oversight includes ensuring that security personnel meet the physical requirements (such as medical) prior to assuming any security duty. The training instructor is typically responsible for the final documentation of each critical task qualification performed by individuals who are assigned duties and responsibilities identified in the Commission-approved security plans.

The requirement for a "qualified" training instructor was added to ensure that the training program is managed and designed to support the site's response strategies and regulatory requirements by an individual who is qualified within the licensee's program and processes to develop, implement and provide oversight of the security training program. The security supervisor shall then verify and attest to the proper documentation and completion of each individual's training record as prepared by the qualified training instructor.

Comment Summary:
Another commenter recommended that, because on-the-job training (OJT) can be signed off by personnel qualified for that task, the Commission should replace "qualified training instructor" with "qualified personnel." The commenter recommended that the Commission revise 10 CFR 73, Appendix B, B.1.b in the final rule to state: "The qualification of each individual to perform assigned duties and responsibilities must be documented *and the security supervisor must attest to the fact that the required training was administered by qualified personnel*."

NRC Response:
The Commission disagrees and has retained the proposed language as written. Although OJT may be conducted by field training officers (FTOs) and/or subject matter experts (SMEs) who may initially verify (sign-off) that a trainee has successfully completed the OJT assignments, the OJT program remains under the control and direction of a qualified security training instructor and the final documentation for the completion of the OJT program must be conducted by the qualified training instructor to ensure all program goals and regulatory requirements are met by the licensee.

Comment Summary:
One commenter recommended that the Commission insert the phrase "of assigned security job duties and responsibilities" at the end 10 CFR 73, Appendix B, B.2.a.(1) in the final rule. The commenter stated that this would allow for use in limited duty positions.

NRC Response:
The Commission agrees. This paragraph is revised to provide the ability to utilize personnel in other capacities within the physical protection program that will not be adversely affected by the current physical condition and qualification of the individual.

Comment Summary:
One commenter stated that the requirements in 10 CFR 73, Appendix B, B.2.a.(1) adequately address the physical requirements for unarmed security personnel. Thus, the commenter recommended that the Commission delete "and unarmed members" from the provision in the final rule.

NRC Response:
The Commission disagrees. Paragraph B.2.a.(1) is the requirement for individuals to not have any physical conditions that would adversely affect their performance, and B.2.a.(2) is the requirement for a physical exam. The physical exam is applicable to any individual assigned to perform physical protection and/or contingency response duties within the physical protection program.

Comment Summary:
One commenter stated that proposed Part 73 Appendix B, B.2.a.(4) is more stringent than existing requirements. The commenter stated that all personnel that have roles and responsibilities in the day-to-day security operations of the facility but little or no responsibility in actual response to contingency events should not be required to meet an increased physical standard. Thus, the commenter recommended that the Commission revise this provision in the final rule by deleting "and unarmed."

NRC Response:
The Commission disagrees. The language states, in part, "as required to effectively perform their assigned duties". This will allow the licensee to evaluate each assigned duty and the minimum physical requirement associated with each assigned duty to ensure that individuals assigned to perform physical protection and/or contingency response duties are physically qualified commensurate with the duties assigned.

Comment Summary:
Another commenter stated that the requirements in 10 CFR 73, Appendix B, B.2.a.(1) adequately address the physical requirements for unarmed security personnel. Also, the commenter noted that there appears to be a error in the numbering sequence that follows 10 CFR 73, Appendix B, B.2.a.(4). Thus, the commenter recommended that the NRC reword this provision to state: "…the licensee protective strategy, and implementing procedures, meets the minimum physical requirements *delineated in B.2.b, B.2.c, and B.2.d* as required to effectively perform their assigned duties."

NRC Response:
The Commission agrees in part. The numbering sequence is revised. The Commission disagrees with the rule text change and has retained the proposed language as written to ensure the text provides the clarity needed when discussing two different requirements that are being addressed by paragraphs B.2.a.(1) and B.2.a.(4).

Comment Summary:
The commenter stated that 10 CFR 73, Appendix B, B.2.b seems unnecessary; the existing requirements ensure the officer has an extra pair of corrective lenses. The commenter argued that the rule language does not need to be so prescriptive to tell the officer when to wear the extra pair of lenses.

NRC Response:
The Commission disagrees. The medical requirements listed in the following paragraphs were taken from pre-existing rule language. No changes were made to these specific requirements.

Comment Summary:
The commenter stated that 10 CFR 73, Appendix B, B.2.f applies to all security personnel.

NRC Response:
The Commission disagrees. This paragraph of the rule applies to any individual that performs physical protection and/or contingency response duties associated with the effective implementation of the Commission-approved security plans, licensee protective strategy, and implementing procedures.

Comment Summary:
Referencing 10 CFR 73, Appendix B, B.3.b, one commenter recommended that the Commission modify this provision by inserting the phrase “or other person professionally trained to identify emotion instability” after “psychiatrist, physician trained in part to identify emotional instability.”

NRC Response:
The Commission disagrees. This would reduce the effectiveness of having a licensed professional conduct the examination.

Comment Summary:
One commenter stated that 10 CFR 73, Appendix B, B.4.a is redundant to B.2.a.(3), which already requires a physical exam by a licensed physician. Thus, the commenter recommended that the Commission delete B.4.a (the first B.4.a).

NRC Response:
The Commission agrees in part, however, no change to the rule text has been made. The physical examination discussed in paragraph B.2.a.(3) of this appendix may be used to fulfill this requirement. The Commission’s expectation is that an individual's current health status is verified prior to engaging in the physical fitness test and that there is no existing medical condition which 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 that is required by 10 CFR 73, Appendix B, B.2.a.(3) provides the verification of the individual's current health status, minimizing the possibility of the individual incurring a medical condition from the time of examination to the time that the physical fitness test is administered.

Comment Summary:
The same commenter stated that the Commission must correct the numbering in 10 CFR 73, Appendix B, B.4.a(1). Thus, the commenter recommended that the NRC replace “from the licensed physician” with “from the exam required by B.2.a.(3).”

NRC Response:
The Commission agrees in part and the numbering sequence error is revised. The second part of the comment is explained in the response above.

Comment Summary:
The commenter stated that 10 CFR 73, Appendix B, B.4.d.(3) should be renumbered to B.4.b.(3).

NRC Response:
The Commission agrees. The numbering sequence is revised.

Comment Summary:
One commenter stated that proposed Part 73 Appendix B, B.4.b.(4) does not allow the use of a trained medical professional or licensed physician to attest to the physical fitness qualification of armed officers who may actually be performing the physical fitness test in a controlled environment. Thus, the commenter recommended that the Commission revise this provision in the final rule to state: "The physical fitness qualification of each armed member of the security organization must be documented by a *licensed medical person, licensed physician, or* qualified training instructor, and attested to by a *licensed medical person, licensed physician, or* security supervisor."

NRC Response:
The Commission disagrees. This would place an unnecessary burden on the medical staff and is not the intent of the rule. The licensed medical professional is required to conduct the medical examination prior to 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 as described in paragraph 10 CFR 73, Appendix B, B.4.a.(1) prior to the test, but is not required to administer the physical fitness test nor are they required to document or attest to the successful completion of the test.

The Commission's expectation is 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 in both normal and emergency operations. The test consists of performing physical activities associated with contingency response duties that replicate site specific conditions which would be encountered in the contingency response environment.

Comment Summary:
Another commenter stated that the Commission should revise 10 CFR 73, Appendix B, B.4.a(1) by replacing "by a qualified training instructor and attested to by a security supervisor" with "and the security supervisor must attest to the fact that physical fitness qualification was administered by qualified personnel."

NRC Response:
The Commission disagrees and has retained the proposed language as written. The Commission has determined that currently, many licensees employ training instructors to manage and direct the oversight of their security training program. The training instructor is typically responsible for the final documentation of each critical task qualification performed by individuals who are assigned duties and responsibilities identified in the Commission-approved security plans.

The requirement for a "qualified" training instructor was added to ensure that the training program is managed and designed to support the site's response strategies and regulatory requirements by an individual who is qualified within the licensee's program and processes to develop, implement and provide oversight of the security training program. The security supervisor shall then verify and attest to the proper documentation and completion of each individual's training record as prepared by the qualified training instructor.

Comment Summary:
One commenter recommended that the Commission revise proposed 10 CFR 73, Appendix B, B.5.a in the final rule by inserting “and alarm station operators” after “armed members of the security organization.”

NRC Response:
The Commission disagrees. The physical examination described in 10 CFR 73, Appendix B, B.2.a.(2) includes alarm station operators whether the alarm station operators are armed or unarmed. This paragraph establishes the requirement for the annual physical requalification (physical examination and physical fitness test as applicable) of any individual assigned to perform physical protection and/or contingency response duties within the physical protection program.

Comment Summary:
One commenter expressed the same concerns for the proposed 10 CFR 73, Appendix B, B.5.b as in B.4.b.(4) above. Thus, the commenter recommended that the Commission revise 10 CFR 73, Appendix B, B.5.b in the final rule to state: “The physical requalification of each armed and unarmed member of the security organization must be documented by a *licensed medical person, licensed physician, or* qualified training instructor and attested to by a *licensed medical person, licensed physician, or* security supervisor.”

NRC Response:
The Commission disagrees. This would place an unnecessary burden on the medical staff and is not the intent of the rule. Once the written medical certification is received by the licensee, it is the Commission’s expectation that the qualified training instructor will document the individual's physical qualification in the individual's training record. The documentation of the physical requalification verifies that the individual has met the basic physical requirements to perform physical protection duties and associated training and qualification activities in accordance with this appendix.

Comment Summary:
Another commenter recommended that the Commission revise the proposed 10 CFR 73, Appendix B, B.5.b in the final rule to state: “The physical requalification of each member of the security organization *and alarm station operators* must be documented *and the security supervisor must attest to the fact that physical requalification was administered by qualified personnel.”*

NRC Response:
The Commission disagrees and has retained the proposed language as written. The Commission has determined that currently, many licensees employ training instructors to manage and direct the oversight of their security training program. The training instructor is typically responsible for the final documentation of each critical task qualification performed by individuals who are assigned duties and responsibilities identified in the Commission-approved security plans.

The requirement for a “qualified” training instructor was added to ensure that the training program is managed and designed to support the site’s response strategies and regulatory requirements by an individual who is qualified within the licensee’s program and processes to develop, implement and provide oversight of the security training program. The security

supervisor shall then verify and attest to the proper documentation and completion of each individual's training record as prepared by the qualified training instructor.

Comment Summary:
One commenter stated that "assigned to perform *any* security-related duty or responsibility," is too broad and should be specific to security-related duties or responsibilities, as identified in the security plans. Thus, the commenter recommended that the NRC revise 10 CFR 73, Appendix B, C.1. by inserting the phrase "as identified in the Commission approved security plans, licensee protective strategy, or implementing procedures" after "duty or responsibility."

NRC Response:
The Commission disagrees. The term "any" is used in conjunction with "security-related duty or responsibility" The Commission believes that this is sufficiently clear and is necessary to establish the appropriate performance-criteria.

Comment Summary:
One commenter recommended that the Commission delete 10 CFR 73, Appendix B, C.1.b.(3) from the final rule because it is redundant to C.1.b.(1). If the Commission does not delete this provision, the commenter recommended that the NRC revise C.1.b.(3) to state: "be trained and qualified in the use of all required equipment or devices required to effectively perform all assigned duties and responsibilities."

NRC Response:
The Commission disagrees. 10 CFR 73, Appendix B, C.1.b.(3)(1) focuses on the training of assigned duties and responsibilities and C.1.b.(3) is to ensure that individuals performing physical protection and/or contingency response duties are not only trained on their assigned duties and responsibilities, but also trained and qualified on the use of all equipment or devices required to effectively perform all assigned duties and responsibilities.

Comment Summary:
One commenter stated that 10 CFR 73, Appendix B, C.2 is new requirement that should be evaluated in the Regulatory Analysis.

NRC Response:
The Commission disagrees. On-the-job training was identified as a new requirement and taken into consideration and discussed in the Regulatory Analysis.

Comment Summary:
The commenter stated 10 CFR 73, Appendix B, C.2.b and C.2.c are not necessary because C.1.a and C.2.a cover these requirements. The commenter also noted that there is a requirement for documentation for OJT in C.2.b that must be moved to C.2.a. Thus, the commenter recommended that the Commission add the following sentence to C.2.a: "On-the-job training must be documented and the security supervisor must attest to the fact that the OJT was administered by qualified personnel."

NRC Response:
The Commission disagrees. The Commission considers the requirement in paragraph 10 CFR 73, Appendix B, C.2.a as minimum criteria that requires licensee's to establish and implement an OJT program to ensure that individuals receive a basic level of "hands on" experience in nuclear security functions before being considered qualified and assigned unsupervised security

duties and responsibilities.

For the requirements outlined in 10 CFR 73, Appendix B, C.2.b and C.2.c, it is the Commission's expectation that the licensee will provide a minimum of 40 hours of OJT specific to contingency response for individuals assigned duties and responsibilities to implement the Safeguards Contingency Plan (armed responders). The OJT provided for contingency response as required by 10 CFR 73, Appendix B, C.2.b and C.2.c is in addition to the OJT required by C.2.a.

The Commission disagrees with the second part of the comment. Although OJT may be conducted by field training officers (FTOs) and/or subject matter experts (SMEs) who may initially verify (sign-off) that a trainee has successfully completed the OJT assignments, the OJT program remains under the control and direction of a qualified training instructor and the final documentation for the completion of the OJT program must be conducted by the qualified training instructor to ensure all program goals and regulatory requirements are met by the licensee.

Comment Summary:
The commenter stated that the Commission should move the elements listed in 10 CFR 73, Appendix B, C.2.c to implementing/regulatory guidance. The commenter stated that the language is too prescriptive for inclusion in a performance-based rule.

NRC Response:
The Commission disagrees. The Commission considers the requirements in 10 CFR 73, Appendix B, C.2.c as minimum criteria needed to ensure armed responders can effectively implement the licensee's protective strategy before being considered qualified and assigned unsupervised security duties and responsibilities associated with contingency response.

Comment Summary:
One commenter stated that proposed 10 CFR 73, Appendix C, Sections II(l) through (l)(6)(iv) do not belong in either Appendix C or the SCP. The commenter stated that the NRC should specify program requirements related to drills and exercises in 10 CFR 73.55 as PSP and T&Q requirement.

NRC Response:
The Commission agrees. The requirements for the performance evaluation program have been relocated to appendix B in entirety as the performance evaluation program and all associated elements are a function of the licensee training and qualification program.

Comment Summary:
Another commenter stated that the Performance Evaluation Program is not a contingency response and the Commission should move these training requirements from the SCP.

NRC Response:
The Commission agrees. See the response above.

Comment Summary:
A commenter noted that the performance evaluation process is a training requirement and is currently described in NEI 03-12, Appendix B, Section 4, Team Training. Also, the commenter stated that the requirements for information provided in the proposed rule are much too detailed

and would be more appropriately placed into regulatory guidance. Thus, the commenter recommended that the NRC eliminate the majority of information and rewriting the proposed rule in a more concise performance-based manner.

NRC Response:
The Commission agrees with relocating the requirements of the performance evaluation program, however, disagrees that the elements within these requirements are too detailed. The Commission believes that the performance evaluation program requirements provide the appropriate level of detail to ensure all program goals and regulatory requirements are met by the licensee.

Comment Summary:
Another commenter stated that the Commission should move all elements of the performance evaluation program to 10 CFR 73, Appendix B, Section C.3. The commenter noted that it is a training requirement and is currently described in NEI 03-12, Appendix B, Section 4, Team Training.

NRC Response:
The Commission agrees. The requirements for the performance evaluation program have been relocated to Appendix B in their entirety as the performance evaluation program and all associated elements are a function of the licensee training and qualification program.

Comment Summary:
A commenter stated that 10 CFR 73, Appendix B, C.3.a does not comply with the EPAct of 2005 because nowhere in this section does it state whether these exercises will be evaluated by the NRC or even if the results of the drills will be required to be submitted to the NRC.

NRC Response:
The Commission does not agree that it is appropriate to place a requirement on the NRC in this rule text. The requirement for the NRC to conduct force-on-force exercises every three years was mandated by Congress and is applicable to the NRC through the EPAct of 2005. The requirements stated in this Appendix apply to NRC licensees.

Comment Summary:
Another Commenter stated that the requirements in 10 CFR 73, Appendix B, Section VI, C.3 do not address Section 651 of the Energy Policy Act of 2005 (EPAct) 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 10 CFR 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.

NRC Response:
The Commission disagrees. Although the Commission has the discretion to issue regulations that govern its own practices (e.g., Part 2), the Commission is not legally required to reflect a statutory 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 (see, e.g., Section 170E

requiring the NRC to conduct a rulemaking to revise the Design Basis Threat), the EPAct 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. If the Commission chooses to limit its compliance with a statutory mandate in the form of specific regulation, then it has the discretion to do so.

The commenter references 10 CFR 73.46(b)(9) (regarding force on force exercises for Category I SSNM fuel cycle facilities) as an example of a regulation that imposes an obligation on the NRC to conduct force-on-force evaluations, and argues that the power reactor regulations should take a consistent approach.

10 CFR 73.46(b)(9), however, does not stand for the proposition claimed by the commenter. This provision requires that "during each 12-month period commencing on the anniversary of the date specified in paragraph (i)(2)(ii) of this section, an exercise must be carried out at least every four 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 regulator imposes an obligation on the licensee to organize and conduct a force-on-force exercise to meet the requirement, and that the licensee must 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.

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 to the Atomic Energy Act of 1954, as amended (AEA), the Commission has conducted over 80 force-on-force inspections at nuclear power plants. In addition, the NRC 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, and does not see the need to codify requirements to impose an obligation on itself to meet this obligation.

Comment Summary:
Regarding 10 CFR 73, Appendix B, C.3.b, one commenter recommended that the Commission delete the word “intercept” because not all sites include interception in their protective strategy.

NRC Response:
The Commission agrees in part. This paragraph is revised to reflect the overall program scope that is the basis for the design and content of implementing procedures for the conduct of tactical response drills and force-on-force exercises. The detailed performance based terminology of “detect, assess, intercept, challenge, delay and neutralize” have been removed from this paragraph and replaced with “demonstrate and assess the effectiveness of the licensee’s physical protection program, protective strategy and contingency event response”.

This revision is necessary to focus the requirement for procedures and their content on the overall scope of the physical protection program, protective strategy and contingency event response and not restrict this requirement to the more detailed sub-elements that support effectiveness. The periodicity requirement for the conduct of tactical response drills and force-on-force exercises is removed from this paragraph as it is captured in paragraph C.3.l(1) of this appendix.

Comment Summary:
One commenter stated that there should be enhanced training of on- and off-site back-up security, and training of both together in realistic scenarios, as well as enhanced and realistic mock-attack drills with requirements to immediately address and fix identified deficiencies.

NRC Response:
The Commission agrees in part, however the conduct of enhanced training with additional on and off site entities is beyond the scope of this rulemaking. The NRC's regulatory authority extends only to licensees and applicants and not to external federal, state and local law enforcement entities. Therefore, the NRC can not mandate external agency participation in such training. It is the licensee's responsibility to ensure that these elements are analyzed and included, if necessary, into their training program.

Paragraph C.3.i of this appendix requires 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 to be entered into the licensee's corrective action program.

Comment Summary:
Another commenter endorsed the recommendations made in previous filings by the Committee to Bridge the Gap and the Union of Concerned Scientists. The commenter urged the Commission to upgrade drills and testing protocols to remedy the flaws that are a matter of public record and to take into account the realities noted herein. The commenter said FOF tests must be sufficiently challenging to provide high confidence in the defensive capabilities of the security forces at the nation's 103 nuclear power plants.

The commenter noted that one clear failing of the FOF program has been excessive warning regarding upcoming tests. While some notice is necessary, the commetner said one week should suffice. In addition, the commenter recommended that staff assignments be frozen on the day of notice, which would eliminate the all too common practice of substituting a plant's most fit and accomplished security personnel in place of underachievers. The commenter stated that it is also critical that drills and the FOF program be revamped to eliminate manifest conflicts of interest. The commenter concluded that the program must be redesigned and monitored by an independent entity such as the U.S. military.

NRC Response:
The NRC FOF program is designed to challenge the licensees protective strategy and measure the licensees capability to provide effective protection against the design basis threat of radiological sabotage. Unlike other FOF exercises conducted by other governmental agencies (DOD, DOE), the NRC is testing the operational readiness of a private entity to defend against the NRC design basis threat. While doing so, the plant is at full operating capacity and the plant must maintain all NRC mandated safety and security requirements.

In order to maintain safety and security compliances, as well as the capability to conduct safe and effective exercises, the Commission has determined that an eight week notification to the licensee meets our requirements to ensure a safe operating environment and an effective and challenging FOF inspection. NRC Inspectors monitor the possibility of personnel substitutions that may detract from a representative sample of the on duty security force. Although there are no regulations prohibiting licensee substitutions of personnel for a force on force inspection,

allegations of substitutions that significantly alter a representative sample are investigated and changes are made to the duty roster if deemed necessary.

The potential for a conflict of interest is addressed in pre-existing NRC regulation as well as in specific elements of the NRC FOF inspection process and is monitored and reviewed to ensure that the potential for a conflict of interest is minimized.

Comment Summary:
One commenter stated that in the context established by 10 CFR 73, Appendix B, C.3.d the rule language should focus on the scope of drills and exercises, not the individual participants. Therefore, the commenter stated that the Commission should revise the provision in the final rule to state: "Drills and exercises must be designed to challenge *the site protective strategy against elements of the design basis threat and ensure participants* demonstrate requisite knowledge, skills, and abilities."

NRC Response:
The Commission agrees with the comment. This paragraph was revised to emphasize the scope and overall objective 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.

Comment Summary:
One commenter stated that the 10 CFR 73, Appendix B, C.3.e requirements are better suited for guidance that currently exists in NEI 03-09.

NRC Response:
The Commission disagrees. The Commission believes that this requirement reflects a performance based criteria that provides a measurable outcome and is appropriate for inclusion in the rule.

Comment Summary:
One commenter stated that the 10 CFR 73, Appendix B, C.3.f requirements are better suited for guidance that currently exists in NEI 03-09. Also, the commenter stated that the term "as needed" is too ambiguous and should be clarified.

NRC Response:
The Commission agrees in part. The Commission believes that this requirement reflects a performance based criteria and is appropriate for inclusion in the rule. This paragraph is revised to clarify that the conduct of drills for training purposes can only be determined by the licensee to address site-specific, individual, or programmatic elements where the licensee has identified a need for improvement or verification.

Comment Summary:
One commenter stated that the 10 CFR 73, Appendix B, C.3.g requirements are better suited for guidance that currently exists in NEI 03-09. Also, the commenter stated that the proposed requirements are more appropriate for exercises than drills. Thus, the commenter recommended that the NRC change the focus to exercises.

NRC Response:
The Commission believes that this requirement is appropriate for inclusion in the rule as it

provides a means to share critique information and program improvements from all levels of drill or exercise participation. The Commission believes that this requirement is applicable to both drills and exercises to provide necessary information for effective performance evaluation and protective strategy improvements.

Comment Summary:
One commenter stated that the 10 CFR 73, Appendix B, C.3.h requirements are better suited for guidance that currently exists in NEI 03-09.

NRC Response:
The Commission disagrees. This section implements the requirements for the documentation of training and qualifications and records prescribed in this appendix.

Comment Summary:
One commenter stated that the 10 CFR 73, Appendix B, C.3.i requirements are better suited for guidance that currently exists in NEI 03-09. Also, the commenter stated that the term "all" is too inclusive and there will be times when the CAP is not the correct avenue to address an issue. Thus, the commenter recommended that the Commission delete this provision from the final rule.

NRC Response:
The Commission agrees in part. The Commission believes that drills and exercises have the potential to identify problems in many areas and that it is important to ensure that all such problems are addressed in a timely manner. The use of the site corrective action program ensures that issues identified can be tracked, addressed and resolved as necessary utilizing an existing licensee process. This paragraph has been revised to remove the term “all’ and to be more explicit to findings, failures and deficiencies that adversely impact the protective strategy and physical protection program.

Comment Summary:
Another commenter stated that 10 CFR 73, Appendix B, C.3.i implies that all findings (good and bad) are required to be entered in the licensee's CAP. The commenter recommended that the NRC amend this section to ensure that only findings that impact the execution or successful implementation of the protective strategy are entered into the CAP, not all findings. Thus, the commenter recommended that the NRC revise the provision to begin as follows "Licensees shall enter all deficiencies and failures that impact the execution or successful implementation of the protective strategy, identified by…"

NRC Response:
The Commission agrees. See the response above.

Comment Summary:
One commenter stated that the 10 CFR 73, Appendix B, C.3.j requirements are better suited for guidance that currently exists in NEI 03-09. Also, the commenter stated that it is not appropriate to assume that all findings or issues need to be protected as SGI. Thus, the commenter recommended that the Commission delete "all" from this provision in the final rule.

NRC Response:
The Commission agrees in part. The Commission agrees that only that information regarding the effectiveness of the physical protection program that meets the criteria of 10 CFR 73.21

needs be protected as SGI. Therefore, this paragraph is revised to include the phrase “as necessary” to delineate the licensees responsibility to review and designate information as SGI in accordance with 10 CFR 73.21. The Commission disagrees that this requirement is better suited for guidance.

Comment Summary:
Similarly, another commenter stated that proposed Part 73 Appendix C, Section II (l)(2)(vi) would require all findings, deficiencies, and failures identified during drills and exercises to be protected as SGI. The commenter argued that this is an unnecessary requirement since not all findings, deficiencies, and failures meet the definition for SGI. For example, the commenter noted that "findings" can be positive versus negative, and identified "deficiencies" are typically immediately corrected/compensated, and thus are not treated as SGI.

In addition, the commenter stated that the reference to 10 CFR 73.21 is not consistent with the new SGI rule published in the Federal Register, dated October 31, 2006. Therefore, the commenter recommended that that the Commission revise this provision in the final rule to state: "Licensees shall protect as safeguards information any uncorrected deficiencies, and failures identified during drills and excercises."

NRC Response:
The Commission agrees in part. See the response above.

Comment Summary:
One commenter stated that the 10 CFR 73, Appendix B, C.3.k requirements are better suited for guidance that currently exists in NEI 03-09.

NRC Response:
The Commission disagrees. The Commission believes that this requirement reflects a performance based criteria that provides a measurable outcome and is appropriate for inclusion in the rule.

Comment Summary:
One commenter stated that 10 CFR 73, Appendix B, C.3.k.(1) is a new requirement that will require all licensees to use MILES gear for all drills and exercises. The commenter said the impact to licensees should be evaluated in the Regulatory Analysis.

NRC Response:
The Commission agrees in part. The use of such equipment is identified in the Regulatory Analysis. The Commission, however, does not specify a methodology or system to meet this requirement.

Comment Summary:
One commenter stated that the 10 CFR 73, Appendix B, C.3.k.(4) requirement is better suited for guidance that currently exists in NEI 03-09.

NRC Response:
The Commission disagrees. The Commission believes that this requirement reflects a performance based criteria that provides a measurable outcome and is appropriate for inclusion in the rule.

Comment Summary:
One commenter stated that 10 CFR 73, Appendix B, C.3.l.(1) is a new requirement for tracking individual participation in drills and exercises. The commenter noted that the security response force is a team effort and individual performance is tracked using the various firearms qualifications.

NRC Response:
The Commission agrees in part. The requirement to conduct quarterly tactical response drills and annual force-on-force exercises is a pre-existing requirement. The Commission's expectation is to ensure that each member of the armed response organization demonstrates the capability to effectively carry-out assigned contingency response duties and responsibilities in accordance with the licensee safeguards contingency plan and protective strategy. The Commission does not consider weapons qualification by itself, to be sufficient to demonstrate this capability and that only through a combination of training, drills, and exercises is this ability adequately demonstrated.

Comment Summary:
Another commenter noted that proposed Part 73 Appendix C, Section II (l)(4)(i) would require all shift personnel to participate in drills and exercises. The commenter argued that, with the existing shift makeup and work-hour restrictions, it would be impossible to comply with this proposed rule as worded. The commenter said quarterly drills and annual exercises are defined as team training in NEI 03-09, and these events are performed independent of individual participation. Thus, the commenter recommended that the Commission revise this provision by adding the phrase "To the extent practicable" to the beginning of the provision in the final rule.

As an alternative, the commenter stated that the provision should read that each member of each shift should participate in a minimum of one quarterly or one annual exercise, on an annual basis. The commenter stated that this ensures that each officer would participate in at least three drills within the three-year training cycle.

NRC Response:
The Commission disagrees with the recommended rule language revision to require participation in these training events "to the extent practicable". The skills associated with the effective implementation of the licensee safeguards contingency plan, protective strategy and contingency response in general are perishable skills that require continual maintenance. The Commission's expectation is to ensure that each member of the armed response organization demonstrates the capability to effectively carry-out assigned contingency response duties and responsibilities in accordance with the licensee safeguards contingency plan and protective strategy. The Commission believes the participation in the training identified in this requirement, by each member of the licensee security response organization, is essential to meet the general performance objective outlined in 10 CFR 73.55(b).

Comment Summary:
One commenter stated that the 10 CFR 73, Appendix B, C.3.l.(2) requirements are better suited for guidance that currently exists in NEI 03-09.

NRC Response:
The Commission disagrees. The Commission believes that this requirement reflects a performance based criteria that provides a measurable outcome and is appropriate for inclusion in the rule.

Comment Summary:
One commenter stated that the final rule should define or describe "NRC observed exercises" to comply with the EPAct. Also, the commenter asked if the requirement to mitigate a conflict of interest only applies to NRC observed exercises, as the language suggests. If so, the commenter stated that this must be changed to include all FOF exercises, not only those evaluated by NRC.

In addition, the commenter stated that that NRC must define the terms "independent" and "direct responsibility" to avoid any ambiguity as to the degree of independence required to satisfy the regulation. In order to avoid this ambiguity, the commenter said the final rule should require that the mock adversaries and plant security officers are not employed by the same security company. This would avoid even the appearance of a conflict of interest, and if properly managed could increase the level of readiness of the plant's security officers.

NRC Response:
The Commission agrees in part. The Commission disagrees that a definition of "NRC observed exercises" is necessary to comply with the EPAct of 2005, as the EPAct of 2005 applies to the NRC not to licensees. Additionally, the Commission disagrees that the provision to avoid a potential conflict of interest is necessary or efficient for exercises other than those conducted during NRC FOF inspections. The Commission believes that exercises conducted during NRC FOF inspections will identify potential flaws that may have not otherwise been revealed by a less aggressive force-on-force testing process.

The terms "independent" and "direct responsibility", as they pertain to this requirement are clarified in regulatory guidance. The Commission disagrees that it is necessary to use an independent security contractor as the mock adversary force for the (licensee supervised) annual force-on-force exercises. Such a requirement would be impractical for licensees to meet given a limited number of resources to choose from and the number of exercises that must be performed.

Comment Summary:
One commenter stated that the 10 CFR 73, Appendix B, C.3.n.(1) requirements are better suited for guidance that currently exists in NEI 03-09.

NRC Response:
The Commission disagrees. The Commission believes that this requirement reflects a performance based criteria that provides a measurable outcome and is appropriate for inclusion in the rule.

Comment Summary:
One commenter stated that proposed 10 CFR 73 Appendix B, D.1.b needs additional clarification to be consistent with current regulatory requirements. Thus, the commenter recommended that the Commission add the following sentences to the end of the provision in the final rule: “The annual written exam content is described in the Commission-approved Training and Qualification plan. The performance demonstration is dependent on the skill/ability being evaluated, and will be at the periodicity defined by the licensee as determined using the Systematic Approach to Training model. In no case shall requalification periods exceed 3 years.”

NRC Response:
The Commission disagrees with the suggested rule text change because the Commission does not intend to require a systematic approach to training for each licensee. It is the Commission's expectation that each licensee is responsible to develop and implement a qualification methodology that includes written exams and performance demonstrations as part of their training program. Written exams and hands-on performance demonstrations provide a means to demonstrate that individuals possess the knowledge, skills and abilities to perform physical protection and/or contingency response duties, whether they choose a systematic approach to training or another acceptable method for implementation of their training program. The periodicity requirements for requalification are clearly outlined in 10 CFR 73, Appendix B, D.2.a. Paragraph D.2.a does not reference or endorse the use of a specific methodology to determine requalification periodicities in lieu of the specified annual requalification.

Comment Summary:
Another commenter recommended that the Commission relocate the requirement for written exam to 10 CFR 73, Appendix B, F.7 because it applies to armed security officers.

NRC Response:
The Commission disagrees. This requirement for written exams includes both armed and unarmed individuals that may be required to perform any assigned security duties and responsibilities and shall be completed prior to assignment.

Comment Summary:
One commenter stated that the 10 CFR 73, Appendix B, D.2.a requirement would be a significant problem and conflicts with the T&Q allowance of a 3-year training cycle. The commenter stated that "shall be requalified at least annually" would preclude the use of the SAT process in determining training program implementation. The commenter argued that the Commission should modify this provision to credit the proper application of the SAT process by each licensee. The commenter recommended that the Commission revise proposed 10 CFR 73, Appendix B, D.2.a by deleting "at least annually" and "this appendix and".

NRC Response:
The Commission disagrees with the comment. The Commission does not intend to require a systematic approach to training (SAT) for each licensee. Therefore, each licensee shall requalify individuals at least annually in accordance with the requirements of this appendix and the Commission-approved training and qualification plan whether they choose an SAT or another acceptable method for implementation of their training program. Though many security duties are performed on a frequent, re-occurring basis, the knowledge, skills and abilities to perform these duties in accordance with established procedures is perishable and must be maintained to meet the requirements of 10 CFR 73.55 (b).

Comment Summary:
The same commenter noted that proposed 10 CFR 73 Appendix B, D.2.b and the associated SOC adds the phrase "by a qualified training instructor." The commenter argued that this blanket addition throughout proposed Appendix B will create a huge administrative burden and add additional cost as processes overseen by other organizations will now require administration by a qualified training instructor.

The commenter stated that the change is apparently an attempt to add value to the training process, but the gain is not apparent. The commenter said that the absence of a definition for

"qualified training instructor" will lead to confusion regarding compliance. The commenter concluded that the current basis for the change does not identify a performance or regulatory gap, so alternate proposals cannot be generated other than to restore the wording to that in the current Appendix B, II.E. The commenter stated that the proposed change creates a regulatory gap where none existed before.

NRC Response:
The Commission disagrees and has retained the proposed language as written. The Commission has determined that currently, many licensees employ training instructors to manage and direct the oversight of their security training program. The training instructor is typically responsible for the final documentation of each critical task qualification performed by individuals who are assigned duties and responsibilities identified in the Commission-approved security plans.

The requirement for a "qualified" training instructor was added to ensure that the training program is managed and designed to support the site's response strategies and regulatory requirements by an individual who is qualified within the licensee's program and processes to develop, implement and provide oversight of the security training program. The security supervisor shall then verify and attest to the proper documentation and completion of each individual's training record as prepared by the qualified training instructor.

Comment Summary:
One commenter recommended that the Commission delete the proposed 10 CFR 73, Appendix B, E.1.b.(1) because this section addresses only the qualifications of fire arms instructors. The commenter noted that those qualifications are articulated in 10 CFR 73 Appendix B, E.1.b.(2), (3), and (4).

NRC Response:
The Commission disagrees. Paragraph E.1.b.(1) describes the minimum requirements for the training and qualification for each armed member of the security organization as it relates to this section of the rule.

Comment Summary:
One commenter stated that 10 CFR 73, Appendix B, E.1.b.(2) is too restrictive and firearms instructor certifications acceptable to law enforcement should be acceptable to the NRC. The commenter stated that the intent is that instructor certification which is adequate for State Highway Patrol, City Police or County Sheriffs, etc. should be acceptable as assurance that licensee firearms instructors will possess the requisite skills to be effective. Thus, the commenter recommended that the Commission revise proposed Part 73 Appendix B, E.1.b.(2) by adding the following sentence to the provision in the final rule: "Certification is acceptable from Colleges and Academies which provide training and certification which is accepted by local/regional law enforcement personnel."

NRC Response:
The Commission agrees in part. The Commission considers law enforcement agencies (regardless of jurisdictional boundary) as a national or state recognized entity. This distinction is made resultant of the standardized doctrine shared throughout the law enforcement community especially at the level of state agencies and below.

The Commission disagrees with the inclusion of a College as meeting the intent for a

recognized national or state entity for licensee's to obtain certification for their firearms instructors. Colleges provide an individual a basic level of instruction for general topics associated to a subject. The Commission's expectation is for firearms instructors to be certified by a national or state recognized entity that has a specific program designed to certify a firearms instructor such as a federal, state or local law enforcement academy or an organization such as the National Rifle Association.

Comment Summary:
One commenter stated that 10 CFR 73, Appendix B, E.1.d is a new requirement that is not consistent with NRC Orders that have been proven adequate for licensee security officers to defend against the DBT. The commenter stated that to remain consistent with existing NRC approved training programs developed to implement the training Order, the Commission should revise this provision so the list is consistent with the Order list. The commenter recommended that the NRC move the list of familiarization elements to 10 CFR 73, Appendix B, E.1.c., then delete E.1.d.

NRC Response:
The Commission disagrees. Most of the elements listed in 10 CFR 73, Appendix B, E. 1.d. are retained from the pre-existing rule and reflect new elements that had been imposed by Commission orders. The additional items listed are not intended to be bound solely by the elements contained in the pre-existing list of the Training Order (April 2003). The additions to the list include the Commission's expectation for training and the experience gained by the NRC 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. This requirement has been revised to reflect accurate language consistent to what is used in the firearms community for the performance elements identified.

Comment Summary:
One commenter stated that 10 CFR 73, Appendix B, E.1.e is not a weapons familiarization training element. The commenter recommended that the NRC place this requirement into the duty training section at Appendix B, C.1.b(4) because it is more appropriate as duty training.

NRC Response:
The Commission agrees in part. The use of deadly force, as authorized by applicable state law, is an assigned duty of armed security personnel and needs to be included in the training program. The Commission disagrees with placing this requirement in another section of the rule based on the Commission's experience that the instruction for the use of deadly force is normally required and conducted during weapons training. Deadly force instruction is more appropriately suited to remain in the weapons training section of the rule versus the duty training section of the rule being that the use of deadly force as intended in this rule is directly related to the use of a weapon and associated training for that weapon.

Comment Summary:
One commenter stated that proposed 10 CFR 73, Appendix B, E.1.f is too prescriptive. The commenter stated that because there is regulatory impact of non-compliance with this activity and time span, licensees need clarification to help ensure compliance. The commenter detailed a suggested approach for range activities, including associated conflictions with the proposed

rule. The commenter stated that 4 months does not appear to have a firm basis, although it is a good "rule of thumb." However, the commenter noted that the problem is the non-compliance that results simply due to a time span that does not clearly relate to a demonstrated performance gap. The commenter acknowledged that the intent of this provision is good, but tracking to this level of detail adds little value while creating significant administrative and personal burden as related to range activities.

Lastly, the commenter stated that "trimester" (4-month period) is not commonly used in the nuclear industry as an interval for other qualification or surveillance activities. Thus, the commenter recommended that the Commission revise this provision in the final rule to state: "Armed members of the security organization shall participate in weapons range activities *to demonstrate that their individual performance continues to support their ability to effectively perform the duties associated with the licensees committed weapon(s). Efforts should be made to have these range activities occur on a nominal 4 month periodicity. An armed responder shall not be considered qualified if they have not fired a licensee approved course of fire within 180 days.*"

NRC Response:
The Commission disagrees. The Commission approved and issued the training order to all power reactor licensees in April of 2003 as a result of the terrorist attacks of September 11, 2001. This requirement is a pre-existing requirement from the training order and is included in the rule. The Commission's intent is to ensure armed members of the security organization maintain an acceptable level of overall proficiency with assigned weapons.

Comment Summary:
Another commenter stated that the Commission should move proposed Part 73, Appendix B, E.1.f to Section F "Weapons Qualification and Requalification."

NRC Response:
The Commission agrees in part. The requirement for range participation on a nominal four month periodicity can include weapons qualification and re-qualification. The Commission disagrees with relocating the text to paragraph F "Weapons Qualification and Re-qualification" being that the Commission's intent for armed members of the security organization participating in weapons range activities, in this paragraph of the rule, is broader than qualification and re-qualification and could include non qualification and re-qualification weapons activities and training.

Comment Summary:
One commenter recommended that the Commission modify 10 CFR 73, Appendix B, F.1.a in the final rule by adding the following phrase to the end of the provision "and the results documented and retained as a record."

NRC Response:
The Commission disagrees with suggested rule text addition by the commenter because 10 CFR 73, Appendix B, F.1.b contains the rule text suggested by the commenter.

Comment Summary:
One commenter recommended that the Commission change the title of 10 CFR 73, Appendix B, F.2, "Firearms Qualification Program" to be consistent with the program described in F.2.

NRC Response:
The Commission disagrees. 10 CFR 73, Appendix B, F.2 is contained within paragraph F which is titled Weapons Qualification and Requalification program.

Comment Summary:
One commenter stated that the requirement for shotgun proficiency has increased by 20 percent above the current requirement with no rationale provided. The commenter argued that the requirement should remain at 50 percent.

NRC Response:
The Commission disagrees. The shotgun qualification score was upgraded from 50 percent in the pre-existing rule, to a score of 70 percent to demonstrate an acceptable level of proficiency which is now reflected in this appendix. The NRC found 70 percent to be a professionally accepted minimum qualification score for day time shotgun proficiency in the firearms training community (local, state and federal law enforcement, National Rifle Association, IALEFI, etc.).

Comment Summary:
One commenter stated that the current NRC-approved industry standard for the qualifying score for the tactical qualification course is 70 percent. The commenter argued that the final rule should be consistent with SFAQ 05-10, approved on December 12, 2005.

NRC Response:
The Commission agrees in part. The current NRC standard of 70 percent for the tactical qualification course is stated in accepted industry and NRC guidance. The Commission, however, disagrees with the current standard of maintaining the 70 percent qualification score for the tactical course of fire. Based on professionally accepted minimum qualification scores for tactical firing proficiency in the firearms training community and the Commission's experience through the implementation of the security baseline inspection program and licensee implementation of the tactical course of fire, the Commission concludes that 80 percent is the minimum acceptable qualification score for the Tactical Qualification Course.

The primary contingency weapon employed by licensees for the success of the protective strategy is the semiautomatic rifle. The qualification courses associated with the semiautomatic rifle require a minimum qualifying score of 80 percent. The Training Order required licensees to develop a tactical course of fire to assess the shooter's physical fitness and the ability to perform realistic and simulated aspects of the sites protective strategy with all contingency equipment. A qualifying score of 80 percent is consistent with the use of the semiautomatic rifle as the primary response weapon and the goal of licensee protective strategies in which a higher degree of accuracy and a greater ammunition capacity is needed to ensure the successful neutralization of the adversarial threat.

The goals of licensee responses to the DBT through the implementation of their protective strategy correlate to the goals of Local, state and federal tactical response teams who typically require response team personnel to demonstrate a level of proficiency greater than 70 percent, due to the critical nature of their mission and to ensure overall success. Most LLEA tactical teams require 80 percent or better, to ensure the neutralization of the threat and the safety of the public through higher accuracy during tactical engagements.

Comment Summary:
One commenter stated that the Commission should change the title of 10 CFR 73, Appendix B,

F.4 to “Weapons Qualifications Courses” because the courses of fire are described in F.3.

NRC Response:
The Commission disagrees. 10 CFR 73, Appendix B, F.4 is specific to the individual courses used to describe the requirements for each course. 10 CFR 73, Appendix B, F.3 outlines the requirement for the specific type of course to be fired with each weapon, i.e. day fire or night fire.

Comment Summary:
One commenter recommended that the Commission remove “and scores” from 10 CFR 73, Appendix B, F.4.a.(1), which are addressed in 10 CFR 73, Appendix B, F.3.

NRC Response:
The Commission agrees. This paragraph has been revised to remove scores as the minimum qualification scores for all weapons are addressed previously in 10 CFR 73, Appendix B, F.3.a, F.3.b and F.3.c.

Comment Summary:
One commenter recommended that the Commission change the title of 10 CFR 73, Appendix B, F.5, to “Firearms Requalification” for consistency.

NRC Response:
The Commission agrees. The title of this paragraph is revised to “Firearms Requalification” to delineate the specific aspect of the physical protection program outlined in this requalification requirement.

Comment Summary:
The commenter recommended that the Commission modify 10 CFR 73, Appendix B, F.5.a by adding the phrase “and the results documented and retained as a record” to the end of the provision.

NRC Response:
The Commission agrees. This requirement is revised to ensure that the results of the requalification efforts are documented and retained as a record in accordance with the documentation and record keeping requirements of this appendix.

Comment Summary:
The commenter stated that cross-reference in 10 CFR 73, Appendix B, F.5.b should be 10 CFR 73, Appendix B, F.4, rather than F.5.

NRC Response:
The Commission agrees. This paragraph is revised to reference the appropriate associated paragraphs within this appendix.

Comment Summary:
The commenter also recommended that the NRC relocate the requirement for written exams from 10 CFR 73, Appendix B, D.1.b to a new Section F.7. The commenter recommended the following language for F.7.1:

"An Annual written exam for armed officers. The written exams must include those elements listed in the Commission approved training and qualification plan and shall require a minimum score of 70 percent to demonstrate an acceptable understanding of assigned duties and responsibilities."

NRC Response:
The Commission disagrees. The requirement for written exams include both armed and unarmed individuals that may be required to perform physical protection and/or contingency response duties and shall be completed prior to assignment. The annual written exam is a qualification requirement specific to armed members of the security organization; however, the content of the exam is not solely based on firearms, therefore it is addressed more appropriately in the "Duty Qualification" paragraph of this appendix.

Comment Summary:
One commenter stated that the proposed Part 73 Appendix B, G.2.b provides a list of required personal protective equipment items for all armed officers, which represents a significant increase in costs to the licensee and is more stringent than current NRC Order requirements. The commenter noted that body armor is not required to be toted, but readily available should the security officer choose to wear it. Therefore, body armor can be pre-staged at assigned response positions and not every security officer is currently required to have their own body armor, as would be required under the proposed rule. In addition, the commenter noted that "duress alarms" are not considered personal equipment required for security officers and should not be listed as such.

The commenter stated that the Commission should limit the list of required equipment for response to contingency events to those personnel that the licensee has listed as responders. The Commission should not require the licensee to provide contingency response equipment for those officers not credited with that type of response. Thus, the commenter recommended that the NRC revise proposed Part 73, Appendix B, G.2.b to state: "The licensee shall provide armed security personnel *with the Commission-approved security plan personal protective equipment.*"

NRC Response:
The Commission agrees, in part. The Commission disagrees that this requirement is more stringent than current requirements, however, agrees with the removal of "duress alarms" from this required equipment list. This paragraph is revised 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 would permit a licensee to pre-stage equipment such as body armor at designated locations consistent with their proactive 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 to 10 CFR 73, Appendix B, G.2.c as an optional piece of equipment that may be made available for use in accordance with the Licensee Protective Strategy and implementation procedures.

Comment Summary:
One commenter stated that proposed 10 CFR 73, Appendix B, G.2.c provides a listing of personal equipment that should be described as optional and required only based on individual

licensee protective strategy requirements. The commenter said the list should strictly be based upon the licensee's specific site protective strategy and this equipment should be provided only if required to successfully implement that protective strategy. In addition, the commenter stated that proposed Item #7 is redundant to Item #2, and the punctuation should be removed from the listing. Therefore, the commenter recommended that the Commission revise 10 CFR 73, Appendix B, G.2.c by inserting "as appropriate" after "should provide," deleting item #7, and deleting the punctuation from the items.

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

Comment Summary:
One commenter, regarding proposed 10 CFR 73, Appendix B, G.3.a, noted that this is a new requirement not in the Orders, EPAct, or NEI 03-12. The commenter stated that the requirement for armorer certification is new, more stringent than current Order requirements, and not well-defined. The commenter stated that the proposed requirement limits licensee flexibility to use experienced personnel.

NRC Response:
The Commission disagrees with the commenter. The Commission's expectation is 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.

Comment Summary:
Another commenter asked, "Who is the certifying body for the armor certifications?"

NRC Response:
The Commission's expectation is 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.

Part 73 Appendix C, Section II
Responses to Public Comments

Comment Summary:
A commenter stated that there should be a requirement for a portable set of truck mounted emergency diesel generators parked far enough away from the site to remain protected by an accidental or deliberate air crash into the reactor site.

NRC Response:
This comment is not within the scope of this rulemaking.

Comment Summary:
A commenter stated that, for existing licensees, the NRC is already deploying a different and more appropriate regulatory scheme for addressing Interim Compensatory Measures (ICM) B.5.b conditions. The commenter stated noted that B.5.b is being controlled with a performance-based license condition that is satisfied by voluntary licensee commitments to B.5.b Phase 2 and Phase 3 mitigating strategies. The commenter argued that this regulatory scheme negates the need for any of the proposed changes or clarifications to Appendix C that cover how the on-site response effort is integrated to provide mitigating strategies that can be effectively implemented under the circumstances associated with loss of large areas of the plant due to explosions or fires. The commenter argued that putting this specific detail in the SCP limits the effectiveness of licensee strategies for dealing with unpredictable plant events. Thus, the commenter stated that the Commission should retain the existing regulatory approach and language.

NRC Response:
The Commission agrees in part. The Commission agrees that the safeguards contingency response plan focuses on the predetermined actions of the site security force and has revised the final rule text to clarify retention of this focus by relocating the requirements pertaining to ICM B.5.b conditions to 10 CFR 50.54(hh) and retaining the requirements specific to safeguards contingency response. The detailed comments pertaining to B5.a, and B.5.b have been relocated to the portion of this document responding to 10 CFR 50.54(hh).

Comment Summary:
The Commission received various comments that recommended that the Commission move all elements of the performance evaluation program of 10 CFR 73, Appendix C to Appendix B, Section C.3.

NRC Response:
The Commission agrees that the performance evaluation program is a component of the training program for security force personnel based on response to contingency events and has relocated the performance evaluation program in it's entirety to 10 CFR 73, Appendix B, C.3. The detailed comments pertaining to the performance evaluation program have been relocated to the comment response document for Part 73, Appendix B.

Comment Summary:
The Commission received various comments that stated the requirement for the threat warning system is a new requirement beyond the scope of the Orders. The commenter noted that the

graduated protective measures were not required by the Security Orders, but were outlined in RIS 2002-12a "NRC Threat Advisory and Protective Measures System" and suggested that these requirements be removed.

NRC Response:
The Commission agrees in part. The requirements pertaining to the threat warning system are new to the rule, however, the industry has been implementing them since they were identified in RIS 2002-12a. The requirements for the threat warning system have been relocated to 10 CFR 73.55(k)(10) as the Commission determined that they were better suited to be addressed as a physical protection program requirement. The detailed comments pertaining to the threat warning system have been relocated to the comment response document for 10 CFR 73.55.

Comment Summary:
A commenter stated that the contingency response plan traditionally focused on the predetermined actions of the site security force, and the proposed changes to Appendix C expand that focus by requiring specifics on non-security response efforts to prevent significant core damage. Further, the commenter stated that the level of detail in the SCP will increase significantly if this rule language stands. Also, the commenter argued that the burden on industry is likely to be quite significant, and this impact was not evaluated in the Regulatory Analysis.

The commenter stated that, in addition to revising the existing plans to incorporate an expanded level of detail, the Commission should add new information such as Memorandum Of Understandings and operational details. In the March 9 public meeting, the Commission indicated that it is not the intent of this section to impose a significant burden on industry. The commenter stated that if it is not the Commission's intent to impose a significant burden on industry, the Commission should revise this section and the existing rule language should only be modified to reflect requirements delineated in the Commissions Orders.

NRC Response:
The Commission agrees in part. The Commission agrees that the safeguards contingency response plan focuses on the predetermined actions of the site security force and has revised the final rule text to clarify retention of this focus. The Commission has determined that the changes to this appendix are consistent with current requirements for the coordination of the predetermined security force actions with those of non-security response efforts to ensure that the predetermined actions of the security force can be effectively implemented without conflict with the predetermined actions of other on-site or off-site support agencies that would be implemented concurrently or simultaneously with the security force actions.

The Commission does not intend that the SCP "include" the details of other site plans, but rather intends to ensure that the security force has considered these other plans and the potential for conflicts have been resolved. The Commission agrees that it is acceptable for the SCP to reference pertinent non-security documents in lieu of "attaching" them to the SCP and has revised this rule text to clarify this intent.

Comment Summary:
Two commenters stated that the details in 10 CFR 73, Appendix C are more stringent than the requirements in 10 CFR Part 73.55 pertaining to security duties and are fundamentally flawed. The commenters noted that this is especially true with respect to preventing core damage. The commenters stated that tying prevention of core damage to security performance confuses the

true security objective of defending target set elements, the loss of which may result in core damage. The commenter argued that this construction is an illogical extension of security responsibility and creates numerous interface issues with operations, emergency planning and other plant procedures and processes.

NRC Response:
The Commission disagrees. As noted by the commenter, the prevention of core damage during a contingency event is initially a function of security which is accomplished through target set protection. Target sets may include operator actions which have the possibility to prevent or mitigate the final outcome of significant core damage. The loss of a target set will likely result in significant core damage, or if a specific target is selected, spent fuel sabotage.

To ensure the effective protection of target sets, which may include operator actions, the Commission has established the prevention of significant core damage and spent fuel sabotage as the criteria to measure the licensee's performance to protect target sets. Significant core damage and spent fuel sabotage can be measured through accepted engineering standards, and provides measurable performance criteria relative to protection against radiological sabotage. Additionally, the terms "significant core damage" and "spent fuel sabotage" are well established and have been used consistently by the Commission and industry relative to force-on-force testing before and after September 11, 2001.

Comment Summary:
One commenter agreed that the security-related requirements from the security Orders should be codified, but stated that the portions of the Orders that are not security-related should not be included in the security rule. The commenter said that the proposed 10 CFR Appendix C too broadly attempts to make the SCP encompass the entire integrated plant response to all postulated events, including those beyond the DBT.

NRC Response:
The Commission agrees in part. The Commission agrees that some of the requirements that were contained in the proposed 10 CFR 73, Appendix C were not the responsibility of the security organization or belong in another area of the rule. This Appendix is revised to remove the requirements pertaining to the performance evaluation program, the specific B.5.a, B.5.b requirements and the requirements pertaining to the threat warning system. This revision also clarifies the focus of the safeguards contingency plan by identifying the specific responsibilities of the licensee security organization in the planning and preparation for the response to contingency events and reflects 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 base: (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 or modified and 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 determined to be better suited for inclusion in 10 CFR 73.55 (k)(10). The proposed rule category of information (9) requirement regarding imminent threat is relocated to the new 10 CFR 50.54(hh)(1). The proposed rule category of information, (10) Performance Evaluation Program, is removed from this appendix in it’s entirety and has been incorporated in 10 CFR 73,

Appendix B as these requirements describe the development and implementation of a training program for training the security force in response to contingency events.

Comment Summary:
One commenter stated that proposed 10 CFR Appendix C, Section II and associated SOCs add a requirement to include additional detailed information in the SCP, exceeding what was required for the post-DBT SCP. The commenter stated that it is unclear, after moving detail from the PSP and SCP to site procedures as part of DBT, why it is now necessary to not only restore but expand detail and move it into the SCP. The commenter argued that this is unnecessary duplication that provides no benefit and will hinder upgrades. Thus, the commenter recommended that the Commission delete the proposed additional requirements for the SCP.

NRC Response:
The Commission agrees in part. This appendix is revised to clarify the level of detail required to be included in the SCP, as well as, the supporting information that must be documented in implementing procedures. The Commission agrees that it is acceptable to reference rather than include specific information that exists in the PSP and has identified those areas, within this appendix, where referencing information in the SCP is acceptable.

Comment Summary:
One commenter stated that current SCPs are focused on events rather than threats, so the change to “threats” would cause considerable rework of the existing SCPs with no benefit to the security of licensee facilities. The commenter argued that the Commission should maintain the existing concept of response to events rather than threats. Thus, the commenter recommended that the Commission revise the provision in the final rule by replacing “threats” with “security related events”.

NRC Response:
The Commission agrees. The Commission agrees that the term “event” is the more appropriate term. An event includes all actions from initiation (detect) to termination (neutralize), therefore, this requirement is revised to focus on the types of actions or information that will prompt the licensee to begin and end response activities as a result of an actual event at the facility.

Comment Summary:
The same commenter stated that, based on a literal reading of the proposed regulation, this section is a new requirement and the Commission should retain the current rule language. If retained, the commenter recommended that the Commission revise this provision by replacing “threat condition” with “security event”.

NRC Response:
See the response above.

Comment Summary:
The commenter also stated that the detailed language within the proposed rule pertaining to the Generic Planning Base does not belong in the Generic Planning Base and thus recommended that the Commission delete this provision from the final rule.

NRC Response:

The Commission agrees in part that the details in the proposed rule pertaining to the Generic Planning Base did not belong under the Generic Planning Base and reflect the required elements of the Responsibility Matrix. The requirements pertaining to the Generic Planning Base have been revised to reflect elements specific to the initiation and termination of events, the goals and objectives of the licensee during these events and the data, criteria, procedures, mechanisms and logistical support necessary to achieve the objectives identified.

Comment Summary:
One commenter stated that 10 CFR 73, Appendix C too broadly attempts to make the SCP encompass the entire integrated plant response to all postulated events including those beyond the DBT. The commenter noted that specific SOC language in the appendix forbids reference to other site procedures ("To the extent that the topics are treated in adequate detail in the licensee's approved physical security plan, they may be incorporated by cross reference to that plan" would be deleted because this information would be required to be specifically detailed in contingency planning" [Section 3(e)]).

NRC Response:
The Commission agrees in part. The Commission agrees that some of the requirements that were contained in the proposed 10 CFR 73, Appendix C were not the responsibility of the security organization and has revised this appendix to remove those requirements. The Commission disagrees that this appendix forbids reference to other documents and has revised the final rule to clarify that it is acceptable to reference rather than include related information that exists in other documents.

Comment Summary:
As a general comment, another commenter stated that the proposed rule uses the words "must include" throughout. The commenter said the repeated use of this statement will significantly increase the level of detail that is placed into the Plans. The commenter noted that the philosophy for updating the plans, which was concurred with by the NRC, was to place implementation details in site procedures. The commenter concluded that it now appears that the proposed rule will result in a great deal of implementation detail being added into the plans unnecessarily.

NRC Response:
The Commission agrees in part. The Commission does not intend to expand the amount of information required to be "included' in the SCP. The Commission agrees that implementing details are appropriate for procedures and need not be included in the SCP, however, the Commission believes that the licensee must provide a sufficient level of detail in the SCP for the information to be understandable. This paragraph is revised to clarify what level of detail must be included in the SCP and what is expected to be specified in licensee implementing procedures.

Comment Summary:
One commenter stated that these requirements are more stringent than the current Orders. The commenter argued that the elements of the on-site physical protection program are adequately addressed with the requirements in 10 CFR 73.55 and are captured by the licensees in their NRC-approved PSPs. Thus, the commenter stated that it is duplicative to have these same elements repeated in the SCPs. The commenter recommended that the Commission delete these requirements from the final rule. If the Commission retains these requirements, the commenter stated that the Commission should provide an adequate basis for doing so.

NRC Response:
The Commission agrees in part. The Commission agrees that these requirements appear to be more stringent than what exists in current Commission orders. This appendix is revised to retain many of the current requirements in 10 CFR 73, Appendix C, incorporate the applicable requirements of the Commission orders, and update the requirements to reflect the Commissions expectation for contingency planning and performance from experience gained by the NRC through nearly 30 years of security program inspections and observations.

This revision is not intended to be bound solely to codifying the current requirements contained in the Commission orders. These requirements are intended to provide the performance-criteria for the SCP and to describe how the physical protection program provides adequate protection through the measures described in both the PSP and SCP. This appendix is revised to clarify the level of detail required to be included in the SCP, as well as, the supporting information that must be documented in implementing procedures. The Commission agrees that it is acceptable to reference rather than include specific information that exists in the PSP and has identified those areas, within this appendix, where referencing information in the SCP is acceptable.

Comment Summary:
One commenter noted that including a description of how command and control will be coordinated and maintained is a level detail contained in site procedures. The commenter argued that performance-based regulation should not be written to the level of detail suggested by this provision. Thus, the commenter recommended that the Commission retain the current language to avoid adding unnecessary detail.

NRC Response:
The Commission disagrees. A description of how command-and-control will be maintained is needed for the understanding of how the licensee contingency response structure is managed during events. The Commission does not intend to require procedure level detail and agrees that it is acceptable to reference rather than include specific information that exists in the PSP and has identified those areas, within this appendix, where referencing information in the SCP is acceptable.

Comment Summary:
Regarding the proposed 10 CFR 73, Appendix C, Section II (e)(2)(I) “physical layout”, one commenter stated that the proposed regulation is too prescriptive. The commenter requested that the Commission provide the regulatory basis for requiring the inclusion of maps and drawings to the level of detail delineated in the proposed rule. The commenter recommended that the Commission retain the current language to avoid adding unnecessary detail.

NRC Response:
The Commission disagrees. The Commission intends to require the level of detail already included in the current NRC-approved security plans and where information is documented in the PSP to comply with the requirements of the PSP (maps and drawings), this information may be identified by reference in the SCP.

Comment Summary:
The commenter stated that the current regulation is adequate. The commenter argued that the proposed language is too prescriptive and will result in a significant amount of work to revise site security plans. Thus, the commenter recommended that the NRC retain the current

language to avoid adding unnecessary detail.

NRC Response:
See the response above.

Comment Summary:
One commenter stated that this provision is too prescriptive and the level of detail regarding number of law enforcement personnel, types of weapons, and response time lines is more appropriate for guidance. Thus, the commenter recommended that the Commission retain the current language regarding law enforcement assistance to avoid adding unnecessary detail. The commenter also stated that this provision is too prescriptive and the level of detail regarding LLEA agreements is more appropriate for guidance. Thus, the commenter recommended that the Commission retain the current language to avoid adding unnecessary detail.

NRC Response:
The Commission agrees in part. The Commission agrees that certain information pertaining to law enforcement (i.e.weaponry, special capabilities etc.) is a level of detail that should be identified in implementing procedures. It is the Commission's expectation that licensees provide a listing of available law enforcement agencies and a general description of their response capabilities and their criteria for response. It is also the Commission's expectation that licensees include a discussion of working agreements or arrangements for communicating with these agencies within the SCP.

Comment Summary:
One commenter stated that for cases where a plant does not have armed security officers, the Commission should revise 10 CFR 73, Appendix C, 3.c.(v) to state: "The licensee shall provide an armed response team consisting of armed responders and armed security officers, to carry out response duties as described in approved security plans".

NRC Response:
The Commission disagrees. This is a general requirement. The licensee must describe the structure and responsibilities of only those personnel (armed responders and armed security officers) that are identified to perform contingency response duties within their Commission-approved security plans.

Comment Summary:
One commenter stated that # 3 in 73, Appendix C, 3.c.(v) implies that each position in the protective strategy would require a bullet resistant rated enclosure (BRE) or shielding. If this is the intent, the commenter said the costs to the licensee could be prohibitive at many facilities. The commenter argued that this requirement should be based upon the impact in successfully implementing the licensee's site protective strategy, and should be clearly defined as such. Thus, the commenter recommended that the Commission revise this provision in the final rule by adding "as described in the Commission-approved security plan" to the end of the provision.

NRC Response:
The Commission agrees in part. This requirement is revised to clarify the Commission expectation for the protective strategy to consider the protection of response personnel. The intent of this requirement is to support the members of the contingency response organization in

their efforts to fulfill their assigned contingency response duties. The utilization of cover provided by existing plant structures, to include the bullet resisting protected positions licensees may incorporate, is conducive to this intent. The Commission believes this requirement (# 3) is appropriately generic and, as stated, does NOT require nor does it "imply" a BRE for every position or member of the Armed Response Team. The Commission believes that this intent is adequately and appropriately represented by the final rule text.

Comment Summary:
Another commenter stated that the final rule should ensure that security officers with duties other than immediate armed response are not required for protection against the DBT and are not inappropriately credited in FOF exercises. The commenter noted that the proposed rule requires that licensees provide an armed response team consisting of both "armed responders" and "armed security officers." The commenter explained that the difference between the two terms is that "armed responders" cannot be assigned "any other duties or responsibilities that could interfere with response duties." "Armed security officers," on the other hand, can be assigned such duties or responsibilities. Therefore, the commenter argued that the Commission should write the final rule to clarify that only "armed responders" can be utilized in the protective strategy to protect against the DBT.

NRC Response:
The Commission agrees in part. This issue is specifically addressed by this final rule in 10 CFR 73.55(k) which requires that licensees document, in the Commission-approved security plans and site protective strategy, the minimum number of armed responders who are inside the protected area and are available at all times to perform response duties. Armed responders may not be assigned other duties. This requirement also allows the licensee to supplement armed responders with armed security officers, who are onsite and available at all times to perform response duties during contingency events, if the armed security officers are trained, qualified and equipped to perform these response duties and the minimum number of armed security officers is specified in the NRC-approved security plans and site protective strategy.

The Commission agrees that because armed security officers are not required for immediate response, they may be assigned other duties. However, if used, the licensee is required to specify the duties that armed security officers will perform within the protective strategy and is responsible for ensuring that other assigned duties, not required by the protective strategy, do not prevent the armed security officers from meeting their response duties and timelines as specified by the protective strategy.

For the purposes of force-on-force testing, a licensee may use less than the documented number of armed responders and armed security officers, but is explicitly prohibited from using more than the minimum number stated in the approved security plans and protective strategy. Therefore, the Commission disagrees with the recommendation to limit a licensee to only utilize armed responders designated in the Commission-approved security plans and site protective strategy to protect against the design basis threat and for the purpose of force-on-force testing.

Comment Summary:
A commenter stated that in the proposed rule the use of the qualifier “all” when referring to describing the types of decisions that must be made during a contingency event is too inclusive and will be impracticable to implement. Thus, the commenter recommended that the NRC revise the provision in 10 CFR 73, Appendix C, 4. by deleting “all”.

NRC Response:
The Commission agrees that the use of “all” in this paragraph to describe all possible decisions to be made regarding a situation is beyond the scope of this requirement. This paragraph is revised to outline the specific events along with identifying the required information regarding associated responsibilities and actions that licensees shall include within their responsibility matrix.

Comment Summary:
Two commenters stated that 10 CFR 73, Appendix C, 5.(i) is not necessary and duplicative of the proposed requirements of 10 CFR 73.55(c)(6)(i).

NRC Response:
The Commission agrees in part. The requirement for implementing procedures exists in each section, or appendix of the rule which appears to be redundant; however, as each section of the rule contains requirements for differing program elements, and to ensure each program element is addressed in a document that demonstrates “how” the licensee accomplishes tasks to meet the Commission regulations, it is necessary to institute a requirement for implementing procedures in each section or appendix of the rule.

Comment Summary:
One commenter stated that proposed 10 CFR 73 Appendix C, Section II, records and reviews is redundant to proposed 10 CFR 73.55 records and review requirements. Thus, the commenter recommended that the Commission delete the proposed 10 CFR 73 Appendix C, Section II records and reviews.

NRC Response:
The NRC agrees in part and has revised this section to clarify the specific elements of the physical protection program that must be reviewed and audited as well as information required to be documented in records. The information that is required to be recorded and reviewed is specific to the safeguards contingency plan as stated in requirements (2) and (3). This revision also included modifying the language of these requirements to be consistent with all physical protection program review and record requirements.

Comment Summary:
A commenter stated that the language in 10 CFR 73 Appendix C, Section II, records and reviews should be consistent with that of Appendix B.I.

NRC Response:
See the response above.

Appendix A:

INCREMENTAL LICENSEE ACTIVITIES AND COST EQUATIONS FOR INDIVIDUAL PROVISIONS OF THE DRAFT FINAL RULE

A.1 SECTION 73.54: ONE-TIME COSTS FOR LICENSEES

Cyber Security Plan

The licensee shall establish, implement, and maintain a Commission-approved cyber security plan.

Note: This calculation accounts for the cost to establish and implement the Cyber Security Plan required by section 73.54(e) of the final rule.

Hours of executive time per plan		4
Labor rate of executive per hour	x	$200
Cost of executive time per plan		*$800*
Hours of manager time per plan		40
Labor rate of manager per hour	x	$150
Cost of manager time per plan		*$6,000*
Hours of staff time per plan		120
Labor rate of staff per hour	x	$100
Cost of staff time per plan		*$12,000*
Hours of clerical time per plan		8
Labor rate of clerical worker per hour	x	$50
Cost of clerical worker time per plan		*$400*
Subtotal cost per plan		*$19,200*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($1,248,000)***

Section 73.54: ONE-TIME COSTS FOR LICENSEES (Continued)

Cyber Security

Licensees must establish cyber security programs to protect important computer systems. This requirement will result in procedures, training, and hardware modifications.

Assessment and program implementation:

Hours of IT Manager time per site		2,000
Labor rate of IT Manager per hour	x	$150
Cost of IT Manager time per site		*$300,000*
Hours of IT Staff time per site		3,000
Labor rate of IT Staff per hour	x	$100
Cost of IT Staff time per site		*$300,000*

Equipment and Installation:

Cost of equipment and installation per site		*$375,000*

Training:

Hours of staff time		1
Labor rate of staff per hour		$100
Number of people requiring training per site	x	2,000
Cost of training per site		*$200,000*
Subtotal cost		*$1,175,000*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($76,375,000)***

A.2 SECTION 73.54: ANNUAL COSTS FOR LICENSEES

Cyber Security

Licensees must establish cyber security programs to protect important computer systems. This requirement will result in ongoing training and equipment maintenance costs.

Hours of staff time		1
Labor rate of staff per hour		$100
Number of people requiring training per site	x	2,000
Cost of training per site		*$200,000*
Cost of cyber security equipment maintenance per site		*$75,000*
Subtotal cost of cyber security staff and equipment maintenance per site		*$275,000*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($17,875,000)***

A.3 SECTION 73.55: ONE-TIME COSTS FOR LICENSEES

Update Plans and Procedures

Licensee must update Physical Security, Training and Qualification, and Safeguards Contingency Plans within 180 days of the effective date of the final rule.

Note: This calculation accounts for revisions to the Plans required by section 73.55(a)(1) of the final rule, along with corresponding revisions to all relevant procedures (but excluding procedures related to Safety/Security Interface, which are costed under 73.58).

Revisions to Plans

Hours of executive time		20
Labor rate of executive per hour	x	$200
Cost of executive time		*$4,000*
Hours of manager time		100
Labor rate of manager per hour	x	$150
Cost of manager time		*$15,000*
Hours of staff time		420
Labor rate of staff per hour	x	$100
Cost of staff time		*$42,000*
Hours of clerical time		20
Labor rate of clerical worker per hour	x	$50
Cost of clerical worker time		*$1,000*
Subtotal cost per site		*$62,000*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Subtotal cost of plans		*($4,030,000)*

Section 73.55: ONE-TIME COSTS FOR LICENSEES (Continued)

Revisions to Procedures

Hours of executive time		20
Labor rate of executive per hour	x	$200
Cost of executive time		*$4,000*
Hours of manager time		100
Labor rate of manager per hour	x	$150
Cost of manager time		*$15,000*
Hours of staff time		420
Labor rate of staff per hour	x	$100
Cost of staff time		*$42,000*
Hours of clerical time		20
Labor rate of clerical worker per hour	x	$50
Cost of clerical worker time		*$1,000*
Subtotal cost per site		*$62,000*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Subtotal cost of procedures		*($4,030,000)*
Subtotal cost of plans		*($4,030,000)*
Subtotal cost of procedures	+	*($4,030,000)*
Total Cost		***($8,060,000)***

Video Capture

The Isolation Zone video surveillance and assessment equipment must be designed to provide real-time and play-back/recorded video images in conjunction with an alarm annunciation in a manner that allows timely assessment of activities prior to and after the alarm annunciation. According to a representative from a video surveillance technology supplier, approximately 70 percent of sites have this technology already in both the CAS and SAS. Therefore, this analysis assumes 30 percent of sites will need to establish this technology in their CAS and SAS.

Note: This calculation accounts for the video technology requirements in section 73.55(e)(5)(i)(C) of the final rule.

Cost to install real-time and play-back/recorded video images in conjunction with alarm annunciation capabilities to the CAS and SAS per site		*$140,000*
Number of sites		*65*
Percentage of sites affected	*x*	*30%*
Total Cost		***($2,730,000)***

Section 73.55: ONE-TIME COSTS FOR LICENSEES (Continued)

Training for Escorts

The licensee must ensure that all escorts meet minimum standards, such as training, access authorization, communication abilities, knowledge of authorized activities, and description of escort-visitor ratios. For the purposes of this regulatory analysis, it is assumed that current training for licensee workers will be revised to include escort training requirements.

Note: This calculation accounts for the escort training requirement set forth in section 73.55(g)(8) of the final rule.

Hours of trainer time to revise training package per site		40
Cost of trainer time per hour	*x*	$100
Cost of trainer time per site		*$4,000*
Subtotal cost per site		*$4,000*
Number of sites		*65*
Percentage of sites affected	*x*	*100%*
Total Cost		***($260,000)***

Two-Way Radios for Escorts

The licensee must ensure that individuals assigned to visitor escort duties shall be provided a means of timely communication with security personnel in a manner that ensures the ability to summon assistance when needed as required by section 73.55(g)(8)(iii) of the final rule.

Number two-way radio units per site		12
Cost per unit	x	$300
Cost of two-way radio units per site		*$3,600*
Subtotal cost per site		*$3,600*
Number of sites		*65*
Percentage of sites affected	*x*	*100%*
Total Cost		***($234,000)***

Section 73.55: ONE-TIME COSTS FOR LICENSEES (Continued)

Escort Communication

Each individual assigned to vehicle escort duties must be capable of maintaining continuous communication with security personnel to ensure the ability to summon assistance when needed as required by section 73.55(g)(8)(ii) of the final rule.

Unit cost of communication resources for escorts		$500
Number of units needed per site	x	60
Cost of escort communication per site		*$30,000*
Subtotal cost per site		*$30,000*
Number of sites		65
Percentage of sites affected	x	*100%*
Total Cost		***($1,950,000)***

Duplicative Capabilities in CAS and SAS

Section 73.55(i)(4)(iii) requires new reactors to construct, locate, protect, and equip both the central and secondary alarm stations to the standards of the central alarm station requirements of 73.55. However, this requirement does not apply to new reactors that use a design certified before the final rule takes effect. For new reactors covered by COL applications that already have been submitted to the NRC, therefore, the NRC staff believes this requirement will not be applicable.

Uninterrupted Power

Licensees must install uninterrupted power to the intrusion detection and assessment system. The analysis assumes that 85 percent of sites already have an uninterrupted power source.

Cost to install uninterrupted power per site		*$500,000*
Number of sites		*65*
Percentage of sites affected	*x*	*15%*
Total Cost		***($4,875,000)***

Section 73.55: ONE-TIME COSTS FOR LICENSEES (Continued)

No Single Act

Licensees must ensure that no single act can disable the functional capabilities of both the CAS and the SAS. Licensees must assess their current configuration, and as needed, make plan changes (alternative measures) or structural modifications. This analysis assumes that 5 percent of sites will require structural modifications to comply with the final rule.

Note: This calculation accounts for assessment and structural modification costs as required by section 73.55(i)(4)(i) of the final rule.

Assessment

Hours of manager time per site		20
Labor rate of manager per hour	x	$150
Cost of manager time per site		*$3,000*
Hours of staff time per site		40
Labor rate of staff per hour	x	$100
Cost of staff time per site		*$4,000*
Cost of manager and staff time per site		*$7,000*
Number of sites		*65*
Percentage of sites affected	*x*	*100%*
Subtotal cost of assessment		*$455,000*

Structural Modifications

Cost of structural modifications		$1,000,000
Number of sites		65
Percentage of sites affected	x	5%
Subtotal cost of structural modifications		*$3,250,000*
Subtotal cost of assessment		*($455,000)*
Subtotal cost of structural modifications	+	*($3,250,000)*
Total Cost		***($3,705,000)***

Section 73.55: ONE-TIME COSTS FOR LICENSEES (Continued)

Target Sets

The licensee must document and maintain the process used to develop and identify target sets, identify and document target set equipment or elements that are not contained within a protected or vital area, and update target set documentation as needed.

Note: This calculation accounts for the costs associated with target set analysis as set forth in sections 73.55(f)(1)-73.55(f)(4) of the final rule.

Hours of manager time per site		120
Labor rate of manager per hour	x	$150
Cost of manager time per site		*$18,000*
Hours of staff time per site		380
Labor rate of staff per hour	x	$100
Cost of staff time per site		*$38,000*
Hours of clerical time per site		60
Labor rate of clerical worker per hour	x	$50
Cost of clerical worker time per site		*$3,000*
Subtotal cost per site		*$59,000*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($3,835,000)***

Section 73.55: ONE-TIME COSTS FOR LICENSEES (Continued)

Heightened Security

Licensees must establish, maintain, and implement a threat warning system.

Note: This calculation accounts for the administrative costs to review the final rule language and to review and revise the existing threat warning system as required by section 73.55(k)(10) of the final rule.

Hours of manager time to review and revise existing system		8
Labor rate of manager per hour	x	$150
Cost of manager time to review and revise existing system		*$1,200*
Hours of legal time to review and revise existing system		20
Labor rate of legal staff per hour	x	$100
Cost of legal time to review and revise existing system		*$2,000*
Hours of staff time to review and revise existing system		40
Labor rate of staff worker per hour	x	$100
Cost of staff time to review and revise existing system		*$4,000*
Hours of clerical time to revise documentation		16
Labor rate of clerical worker per hour	x	$50
Cost of clerical time to revise documentation		*$800*
Subtotal cost per site		*$8,000*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($520,000)***

A.4 SECTION 73.55: ANNUAL COSTS FOR LICENSEES

Target Sets

The licensee must document and maintain the process used to develop and identify target sets, identify and document target set equipment or elements that are not contained within a protected or vital area, and update target set documentation.

Note: The final rule requires licensees to maintain the target set analysis as set forth in sections 73.55(f)(1)-73.55(f)(4) every three years. This calculation presents the annual cost to maintain the target set analysis.

Hours of manager time per site		20
Labor rate of manager per hour	x	$150
Cost of manager time per site		*$3,000*
Hours of staff time per site		80
Labor rate of staff per hour	x	$100
Cost of staff time per site		*$8,000*
Hours of clerical time per site		16
Labor rate of clerical worker per hour	x	$50
Cost of clerical worker time per site		*$800*
Subtotal cost per site		*$11,800*
Number of sites		*65*
Percentage of sites affected per year	x	*33%*
Total Cost		***($253,110)***

Section 73.55: ANNUAL COSTS FOR LICENSEES (Continued)

Escort of Vehicles

Vehicles operated by an individual with unescorted access to the protected area or vital area no longer need a security escort.

Note: This calculation accounts for a relaxation in section 73.55(g)(5)(ii) of the final rule relative to current requirements for escorts.

Number of vehicles entering the protected area operated by an individual with unescorted access per year per site		400
Number of hours spent per escorted vehicle	x	1.5
Number of security escort hours needed per year per site		*$600*
Labor rate of security escort per hour		$25
Number of security escort hours needed per year per site	x	600
Savings due to security escort requirement relaxation per site		*$15,000*
Subtotal savings per site		*$15,000*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Savings		***$975,000***

A.5 SECTION 73.56: ONE-TIME COSTS FOR LICENSEES

Individuals Subject to Authorization Program

Licensees must subject any individual whose assigned duties and responsibilities permit the individual to take actions by electronic means, either on site or remotely, that could adversely impact a licensee's or applicant's operational safety, security, or emergency response capabilities to an authorization program and background check.

Note: This calculation accounts for the initial costs associated with section 73.56(b)(1)(ii).

Number of individuals needing background checks		10
Number of hours to conduct a background check		6
Labor rate of manager per hour	x	$150
Cost of background check per site		*$9,000*
Subtotal cost per site		*$9,000*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($585,000)***

Increased Sharing of Medical Records

Licensees, applicants, and contractors or vendors must develop procedures to provide communication between the licensed psychologist or psychiatrist and other medical personnel.

Note: This calculation accounts for the cost to develop procedures for communication between medical personnel as required by section 73.56(e)(5).

Hours of manager time per site		16
Labor rate of manager per hour	x	$150
Cost of manager time per site		*$2,400*
Hours of legal time per site		16
Labor rate of legal staff per hour	x	$100
Cost of legal time per site		*$1,600*
Hours of staff time per site		40
Labor rate of staff worker per hour	x	$100
Cost of staff time per site		*$4,000*
Hours of clerical time per site		8
Labor rate of clerical worker per hour	x	$50
Cost of clerical time per site		*$400*
Subtotal cost per site		*$8,400*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($546,000)***

Section 73.56: ONE-TIME COSTS FOR LICENSEES (Continued)

Development of Psychological Test Thresholds

A licensed psychiatrist or psychologist must develop thresholds for the psychological test. These predetermined thresholds will be applied in interpreting the test results to determine whether an individual must be interviewed by a licensed psychiatrist or psychologist.

Note: This calculation accounts for the costs for a licensed psychiatrist or psychologist to develop thresholds for each psychological test, as required by section 73.56(e)(3) of the final rule.

Number of psychologists to develop test thresholds per site		1
Number of hours needed to develop test thresholds		20
Labor rate of psychologist per hour	x	$150
Cost to develop test thresholds		$3,000
Subtotal cost per site		*$3,000*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($195,000)***

Section 73.56: ONE-TIME COSTS FOR LICENSEES (Continued)

5-Year Update of Psychological Assessments

The licensee, applicant, contractor, or vendor must administer a psychological reassessment to individuals who perform duties that are critical to the safety and security of the nuclear power plant, and whose initial psychological assessment occurred five or more years ago. Although licensees implemented this requirement with the Order, the analysis assumes that 35 additional individuals per site will require updated psychological assessments.

Note: This calculation accounts for the initial cost to administer a psychological test every five years as required by section 73.56(i)(1)(v)(B).

Number of managers per site who perform duties critical to the safety and security of the nuclear power plant in need of updated psychological assessment		10
Labor rate of manager per hour		$150
Number of hours to complete the test	x	2
Cost of manager time to complete psychological test per site		*$3,000*
Number of staff per site who perform duties critical to the safety and security of the nuclear power plant in need of updated psychological assessment		25
Labor rate of staff per hour		$100
Number of hours to complete the test	x	2
Cost of staff time to complete psychological test per site		*$5,000*
Total number of individuals per site who perform duties critical to the safety and security of the nuclear power plant in need of updated psychological assessment		35
Cost of purchasing test per person	x	$73
Cost of purchasing psychological test per site		*$2,538*
Number of psychologists to adminster, score, and interpret tests on site		1
Number of hours needed to gain training for the test and to administer and score the test		50
Labor rate of psychologist per hour	x	$150
Cost of training required to administer and score test		*$7,500*
Subtotal cost per site		*$18,038*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($1,172,438)***

A.6 SECTION 73.56: ANNUAL COSTS FOR LICENSEES

Records

The licensee must document and retain records relating to an individual's unescorted access authorization status and written agreement of services.

Note: This calculation accounts for the records management activities required by sections 73.56(o).

Hours of staff time		460
Labor rate of staff per hour	x	$100
Cost of staff time		*$46,000*
Hours of clerical time		200
Labor rate of clerical worker per hour	x	$50
Cost of clerical time		*$10,000*
Subtotal cost per site		*$56,000*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($3,640,000)***

Individuals Subject to Authorization Program

Licensees must subject any individual whose assigned duties and responsibilities permit the individual to take actions by electronic means, either on site or remotely, that could adversely impact a licensee's or applicant's operational safety, security, or emergency response capabilities to an authorization program and background check.

Note: This calculation accounts for the access authorization program requirements set forth in section 73.56(b)(1)(ii).

Number of new hires per year needing background checks		5
Number of hours to conduct a background check		6
Labor rate of manager per hour	x	$150
Cost of background check per site		*$4,500*
Subtotal cost per site		*$4,500*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($292,500)***

Section 73.56: ANNUAL COSTS FOR LICENSEES (Continued)

Administration of Psychological Assessments (Tests and Interviews)

Any individual applying for unescorted access or unescorted access authorization status must complete a psychological assessment prior to receiving unescorted access or certified unescorted access authorization. The assessment must include a standardized test in all cases, and must include a clinical interview for individuals who perform job functions that are critical to safety and security. The analysis assumes that licensees already conduct standardized tests for new employees; however, after the final rule becomes effective, they face an incremental cost to hire an APA-licensed professional to conduct the tests. Furthermore, although the Order already requires licensees to administer psychological assessments, the analysis assumes that there are 7 new hires per year that require clinical interviews conducted by an APA-certified professional.

Note: This calculation accounts for the costs to administer and score a psychological test and perform clinical interviews, as required by section 73.56(e) of the final rule.

Tests

Number of psychologists to adminster and score the tests on site		1
Number of hours needed to administer and score the tests		104
Labor rate of psychologist per hour	x	$150
Cost to administer and score the tests		($15,600)
Subtotal cost per site		*($15,600)*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Subtotal cost of tests		*($1,014,000)*

Section 73.56: ANNUAL COSTS FOR LICENSEES (Continued)

Clinical Interviews

Number of managers per site who perform duties critical to the safety and security of the nuclear power plant in need of an interview		2
Number of hours needed per interview		0.5
Labor rate of manager per hour	x	$150
Cost of manager time to complete interviews		$150
Number of staff per site who perform duties critical to the safety and security of the nuclear power plant in need of an interview		5
Number of hours needed per interview		0.5
Labor rate of staff per hour	x	$100
Cost of staff time to complete interviews		$250
Number of psychologists needed to perform interviews		1
Number of hours needed for interviews		7
Labor rate of psychologist per hour	x	$150
Cost of psychologist time to perform interviews		$1,050
Subtotal cost per site		*$1,450*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Subtotal cost of interviews		*($94,250)*
Subtotal cost of tests		*($1,014,000)*
Subtotal cost of interviews	+	*($94,250)*
Total Cost		***($1,108,250)***

Section 73.56: ANNUAL COSTS FOR LICENSEES (Continued)

5-Year Update of Psychological Assessments

The licensee, applicant, contractor, or vendor must administer a psychological reassessment to individuals who perform duties that are critical to the safety and security of the nuclear power plant, and whose initial psychological assessment occurred five or more years ago. Although licensees implemented this requirement with the Order, the analysis assumes that 35 additional individuals will be subject to updated psychological assessments, and that one-fifth of them (7 individuals) require updated psychological assessments per year.

Note: This calculation accounts for the initial cost to administer a psycholoigcal test every five years as required by section 73.56(i)(1)(v)(B).

Number of managers per site per year who perform duties critical to the safety and security of the nuclear power plant in need of updated psychological assessment		2
Labor rate of manager per hour		$150
Number of hours to complete the test	x	2
Cost of manager time to complete psychological test per site		*$600*
Number of staff per site per year who perform duties critical to the safety and security of the nuclear power plant in need of updated psychological assessment		5
Labor Rate of staff per hour		$100
Number of hours to complete the test	x	2
Cost of staff time to complete psychological test per site		*$1,000*
Number of individuals per site per year who perform duties critical to the safety and security of the nuclear power plant in need of updated psychological assessment		7
Cost of purchasing test per person	x	$73
Cost of purchasing psychological test per site		*$508*
Number of psychologists to adminster, score, and interpret tests on site		1
Number of hours needed to administer and score the test		7
Labor rate of psychologist per hour	x	$150
Cost of training required to administer and score test		*$1,050*
Subtotal cost per site		*$3,158*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($205,238)***

A.5 SECTION 73.58: ONE-TIME COSTS FOR LICENSEES

Safety/Security Interface

The licensee must assess and manage adverse effects on safety and security when implementing changes to plant configurations, facility conditions or security. The licensees will need to review and update existing procedures to reference the safety-security interface requirements, as well as revise and update the corresponding guidance documents.

Note: This calculation accounts for the safety-security interface activities required by section 73.58 of the final rule.

Develop and Implement Safety-Security Interface Procedures and Provide Initial Training:

Hours of manager time		100
Labor rate of manager per hour	x	$150
Cost of manager time		*$15,000*
Hours of staff time		220
Labor rate of staff per hour	x	$100
Cost of staff time		*$22,000*
Hours of legal time		80
Labor rate of legal staff per hour	x	$100
Cost of legal time		*$8,000*
Hours of clerical time		40
Labor rateof clerical worker per hour	x	$50
Cost of clerical time		*$2,000*
Number of managers attending initial safety-security interface training		40
Number of hours in training		8
Labor rate of manager per hour	x	$150
Cost of manager time for training per site		*$48,000*
Subtotal cost per site		*$95,000*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Subtotal cost of developing procedures and providing initial training		*($6,175,000)*

Section 73.58: ONE-TIME COSTS FOR LICENSEES (Continued)

Review and Update Existing Procedures:

Hours of manager time		20
Labor rate of manager per hour	x	$150
Cost of manager time		*$3,000*
Hours of staff time		60
Labor rate of staff per hour	x	$100
Cost of staff time		*$6,000*
Hours of legal time		20
Labor rate of legal staff per hour	x	$100
Cost of legal time		*$2,000*
Hours of clerical time		20
Labor rate of clerical worker per hour	x	$50
Cost of clerical time		*$1,000*
Subtotal cost per site		*$12,000*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Subtotal cost of reviewing/updating existing procedures		*($780,000)*

Section 73.58: ONE-TIME COSTS FOR LICENSEES (Continued)

Revise and Update Guidance Documents:

Hours of manager time		20
Labor rate of manager per hour	x	$150
Cost of manager time		*$3,000*
Hours of staff time		40
Labor rate of staff per hour	x	$100
Cost of staff time		*$4,000*
Hours of legal time		20
Labor rate of legal staff per hour	x	$100
Cost of legal time		*$2,000*
Hours of clerical time		10
Labor rate of clerical worker per hour	x	$50
Cost of clerical time		*$500*
Subtotal cost per site		*$9,500*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Subtotal cost of reviewing/updating guidance documents		*($617,500)*
Subtotal cost of developing procedures and providing initial training		($6,175,000)
Subtotal cost of reviewing/updating existing procedures		($780,000)
Subtotal cost of reviewing/updating guidance documents	+	*($617,500)*
Total Cost for Safety/Security Interface		***($4,777,500)***

A.6 SECTION 73.58: ANNUAL COSTS FOR LICENSEES

Safety/Security Interface

The licensee must assess and manage adverse effects on safety and security when implementing changes to plant configurations, facility conditions or security. To accomplish this, the licensee will need to analyze issues that would require management and assessment on an ongoing basis.

Note: This calculation accounts for the safety-security interface activities required by section 73.58 of the final rule.

Number of SSI issues that would require management and assessment per year		100
Number of staff hours of analysis per issue		4
Labor rate of staff per hour	x	$100
Cost of staff analysis of issues that would require management and assessment		*$40,000*
Subtotal cost per site		*$40,000*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($2,600,000)***

A.9 PART 73, APPENDIX B: ONE-TIME COSTS FOR LICENSEES

Physical/Medical Examinations for Security Personnel

The licensee must ensure that all current security personnel who are assigned duties and responsibilities associated with detection, assessment, and response to unauthorized activities (not just the armed personnel) meet minimum vision, hearing, medical, and physical fitness qualifications.

Cost per physical and medical examination		$400
Number of unarmed members of the security organization hired per year per site	x	20
Cost of physical and medical examinations per year per site		*$8,000*
Hours of clerical time per site		40
Cost of clerical time per hour	x	$50
Cost of clerical time per site		*$2,000*
Subtotal cost per site		*$10,000*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($650,000)***

On-The-Job Training

The licensee must develop on-the-job training plans and procedures. The analysis assumes that none of the reactor sites are currently documenting on-the-job training.

Note: This calculation accounts for the costs of on-the-job training program development, as required by Appendix B, section C.2.b of the final rule.

Number of hours for a training manager to develop an on-the-job training plan and program		120
Labor rate of training manager	x	$50
Cost of on-the-job training documentation and certification per site		*$6,000*
Subtotal cost per site		*$6,000*
Number of sites		*65*
Percentage of sites affected	*x*	*100%*
Total Cost		***($390,000)***

Appendix B: ONE-TIME COSTS FOR LICENSEES (Continued)

Qualification of Security Instructors

The licensee must ensure that all security instructors receive required training to qualify them for their duties.

Cost of training per instructor		$1,500
Number of instructors per site	x	4
Cost of training per site		*$6,000*
Subtotal cost per site		*$6,000*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($390,000)***

Armorer Certification

Each licensee shall implement a firearms maintenance and accountability program that includes armorer certification as required by Appendix B, section G.3.a. of the final rule.

Cost of training per staff person		$3,200
Number of staff requiring training per site	x	2
Cost of training per site		*$6,400*
Subtotal cost per site		*$6,400*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($416,000)***

A.10 PART 73, APPENDIX B: ANNUAL COSTS FOR LICENSEES

Physical/Medical Examinations for Security Personnel

The licensee must ensure that all newly hired security personnel who are assigned duties and responsibilities associated with detection, assessment, and response to unauthorized activities (not just the armed personnel) meet minimum vision, hearing, medical, and physical fitness qualifications.

Cost per physical and medical examination		$400
Number of unarmed members of the security organization hired per year	x	5
Cost of physical and medical examinations per year per site		*$2,000*
Hours of clerical time per site		10
Cost of clerical time per hour	x	$50
Cost of clerical time per site		*$500*
Subtotal cost per site		*$2,500*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($162,500)***

Physical Requirements for Security Organization Personnel

The licensee must ensure that armed and unarmed members of the security organization must meet physical requirements annually. Current requirements require just armed members to meet these standards.

Cost of updating physical examination per person		$150
Number of unarmed members of the security organization per site	x	20
Cost of updating physical examination for unarmed members of the security organization per site		*$3,000*
Hours of clerical time per site		20
Cost of clerical time per hour	x	$50
Cost of clerical time per site		*$1,000*
Subtotal cost per site		*$4,000*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($260,000)***

Appendix B: ANNUAL COSTS FOR LICENSEES (Continued)

On-the-Job Training

The licensee must provide 40 hours of on-the-job training to each new member of the armed and unarmed security organization prior to his or her assignment and that licensees currently provide 20 hours of on-the-job of training to each individual. This analysis estimates that there are approximately 12 newly hired armed and unarmed members of the security organization every year. In addition, training managers must document and certify on-the-job training. The analysis assumes that none of the reactor sites are currently documenting on-the-job training; therefore, 100 percent of reactor sites must complete this documentation and certification.

Number of newly hired armed and unarmed members of the security organization per year		12
Number of additional on-the-job training hours per person		20
Labor rate of armed and unarmed security organziation member per hour	x	$25
Cost of additional training for newly hired armed and unarmed security organization members per site		*$6,000*
Number of hours for a training manager to document and certify on-the-job training per year		20
Labor rate of training manager	x	$50
Cost for on-the-job training documentation and certification per site		*$1,000*
Subtotal cost per site		*$7,000*
Number of sites		*65*
Percentage of sites affected	*x*	*100%*
Total Cost		***($455,000)***

Qualification of Security Instructors

The licensee must ensure that all security instructors receive requalification training every three years. For the purposes of this analysis it is assumed that instructors attend a three-day requalificaton training every three years. To estimate the annual cost, this analysis assumes there is one day of requalification training each year.

Cost of training per instructor per year		$250
Number of instructors per site	x	4
Cost of training per year per site		*$1,000*
Subtotal cost per site		*$1,000*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($65,000)***

Appendix B: ANNUAL COSTS FOR LICENSEES (Continued)

Drill Exercise

Licensees must train staff in accordance with the drill exercise requirements of the final rule, as set forth in Appendix B, section C.3. Although the Order already requires licensees to conduct drill exercises, this analysis conservatively assumes that the cost of conducting four six-hour drills per year is entirely attributable to the final rule.

Number of managers participating in each drill		15
Labor rate of managers per hour		$150
Number of drills per year (all shifts)		4
Number of hours per drill	x	6
Cost of manager time to participate in drill exercises per site		*$54,000*
Number of staff participating in each drill		55
Labor rate of staff per hour		$100
Number of drills per year (all shifts)		4
Number of hours per drill	x	6
Cost of staff time to participate in drill exercises per site		*$132,000*
Subtotal cost per site		*$186,000*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($12,090,000)***

Armorer Certification

Each licensee shall implement a firearms maintenance and accountability program that includes armorer certification as required by Appendix B, section G.3.a. of the final rule. The rule requires each armorer to receive one week of training per weapon every three years. The analysis assumes there are two armorers per site with two weapons each.

Cost of training per armorer per weapon per year		$3,200
Number of armorers requiring training per site		2
Number of weapons trainings per armorer	x	2
Cost of training courses per year per site		*$12,800*
Number of armorers per site		2
Hours of training per armorer per weapon per year		40
Number of weapons per armorer		2
Labor rate of armorers per hour	x	$100
Cost of training time per year per site		*$16,000*
Subtotal cost per site		*$28,800*
Number of sites		*65*
Percentage of sites affected per year	x	*33%*
Total Cost		***($617,760)***

A.11 PART C, APPENDIX C: ONE-TIME COSTS FOR LICENSEES

None.

A.12 PART 73, APPENDIX C: ANNUAL COSTS FOR LICENSEES

None.

Appendix B:

INCREMENTAL NRC ACTIVITIES AND COST EQUATIONS FOR INDIVIDUAL PROVISIONS OF THE DRAFT FINAL RULE

B.1 SECTION 73.54: ONE-TIME COSTS FOR NRC

Review Cyber Security Plan

NRC must review and approve licensees' Cyber Security Plans.

Note: This calculation accounts for NRC approval of a cyber security plan as required under section 73.54 of the final rule.

Hours of NRC staff time		100
Labor rate of NRC staff per hour	x	$100
Cost of NRC staff time		*$10,000*
Hours of NRC clerical time		3
Labor rate of NRC clerical worker per hour	x	$40
Cost of NRC clerical worker time		*$120*
Subtotal cost per site		*$10,120*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($657,800)***

B.2 SECTION 73.54: ANNUAL COSTS FOR NRC

None.

B.3 SECTION 73.55: ONE-TIME COSTS FOR NRC

Implementation Guidelines and Inspection Procedures

NRC must revise implementation guidelines and inspection procedures for onsite physical protection systems.

Hours of NRC executive time for implementation guideline and inspection procedure revisions		8
Labor rate of NRC executive per hour	x	$200
Cost of NRC executive time		$1,600
Hours of NRC manager time for implementation guideline and inspection procedure revisions		40
Labor rate of NRC manager per hour	x	$150
Cost of NRC manager time		$6,000
Hours of NRC staff time for implementation guideline and inspection procedure revisions		200
Labor rate of NRC staff per hour	x	$100
Cost of NRC staff time		$20,000
Hours of NRC legal time for implementation guideline and inspection procedure revisions		20
Labor rate of NRC legal staff per hour	x	$100
Cost of NRC legal time		$2,000
Hours of NRC clerical time for implementation guideline and inspection procedure revisions		8
Labor rate of NRC clerical per hour	x	$40
Cost of NRC clerical time		$320
Subtotal cost per site		*$29,920*
Number of sites		*65*
Percentage of sites affected	x	*100%*
Total Cost		***($1,944,800)***

B.4 SECTION 73.55: ANNUAL COSTS FOR NRC

None.

Environmental Assessment Supporting Final Rule: Power Reactor Security Requirements

U.S. Nuclear Regulatory Commission
Office of Nuclear Reactor Regulation

June 2008

UNITED STATES NUCLEAR REGULATORY COMMISSION

ENVIRONMENTAL ASSESSMENT AND FINDING OF

NO SIGNIFICANT IMPACT

The U.S. Nuclear Regulatory Commission (NRC) is amending the security requirements for nuclear power reactors. The security requirements being amended by the power reactor security rulemaking are: § 73.55, § 73.56, 10 CFR part 73, appendix B, and 10 CFR part 73, appendix C. Additionally, the NRC is adding three new requirements to Parts 50 and 73 respectively: § 50.54(hh), § 73.54, and § 73.58. Finally, the rulemaking makes conforming changes to other sections of part 73, part 72, part 50, and part 52 to 1) ensure that cross-referencing between the various security regulations in part 73 is preserved, 2) implement cyber security plan submittal requirements, and 3) preserve requirements for licensees who are not within the scope of this rule.

Historical Background and Overview

The basis for this rulemaking has been derived from several sources. First, prior to the events of September 11th, the NRC had already undertaken an effort to revise its existing security regulations in part 73, as noted in SECY-01-0101 (June 4, 2001). The existing security regulations in part 73 have not been substantially revised for nearly 30 years. After September 11th, that rulemaking effort was delayed for obvious reasons, but the need to reorganize, improve and update the existing security regulations persists. This rulemaking built upon the efforts of the prior rulemaking.

Second, following the terrorist attacks on September 11, 2001, the NRC 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 for 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 security orders that were issued to licensees were:

- 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 NRC completed its review and approval of all 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, in general the enhancements resulted in such measures 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.

Finally, 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, which added Section 161A. to the Atomic Energy Act of 1954, as amended (AEA), concerns use of an expanded arsenal of weapons, including machine guns and semi-automatic assault weapons by NRC licensees as well as imposing certain requirements for fingerprint-based firearms background checks. As noted below, because of considerations that have arisen during the course of this rulemaking, the final rule no longer specifically addresses any provisions of the EPAct of 2005.

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, 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, 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.

Proposed Rule Background

Recipients of the post-September 11th orders were notified that the requirements in those orders were considered interim measures, and that the NRC ultimately intended to reassess those requirements and undertake a rulemaking that would codify generically-applicable security requirements and revise the Commission's existing security regulations. To that end, on October 26, 2006, the Commission issued the proposed Power Reactor Security Rulemaking (71 FR 62664). 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 (72 FR 480 and 72 FR 8951), eventually closing on March 26, 2007. The NRC received 48 comment letters. In addition, the NRC held two public meetings in Rockville, MD, and Las Vegas, NV on November 15 and 29, 2006, respectively, to solicit public comment. The NRC held a third public meeting on March 9, 2007, to facilitate stakeholder understanding of the proposed rule requirements and thereby result in more informed comment 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 NRC 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 (71 FR 62666-62667). Further, the proposed rule also incorporated provisions of the EPAct of 2005, as described above. Most of these new requirements are now reflected in this final rule.

The NRC 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 NRC 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 section 50.54 in the final rule.

Three petitions for rulemaking were also considered as part of the power reactor security rulemaking, consistent with the resolution and closure process for the subject petitions (PRM-50-80, PRM-73-11, and PRM-73-13). Refer to section II of the final rule *Federal Register* notice for a discussion of the NRC's consideration of the petitions.

Significant New Requirements in the Final Rule

The final power reactor security rulemaking contains a number of significant new requirements (versus the requirements currently in the Code of Federal Regulations) listed below:

a. Safety/Security interface requirements. These requirements are located in new section 73.58. The safety/security interface requirements explicitly require licensee to manage and assess the potential adverse interactions 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, a Petition for Rulemaking (PRM 50-80) that requested the establishment of regulations governing proposed changes to the facilities which could adversely affect the protection against radiological sabotage.

b. 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 for the protection of the MOX fuel 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 low plutonium content and the weight and size of the MOX fuel assemblies, is unnecessary to provide adequate protection for this material. The MOX fuel security requirements are consistent with the approach implemented at Catawba Nuclear Station through the MOX lead test assembly effort in 2004.

c. 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 operating license include a cyber security plan, the rule will also require currently operating licensees to submit a cyber security plan to the NRC for review and approval by way of license amendment pursuant to 10 CFR § 50.90 within 180 days of the effective date of this rule. In addition, applicants who have submitted an application for an operating license or combined operating license currently under review by the NRC 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.

d. Mitigative strategies and response procedures for potential or actual aircraft attacks. These requirements are set forth in new paragraph 50.54(hh). Paragraph 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 aircraft or actual threat to a nuclear power reactor facility. Paragraph 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. 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.

e. Access authorization enhancements. Section 73.56 has been substantially revised to incorporate lessons learned from the Commission's implementation of the order requirements, and to improve the integration of the access authorization and security program requirements. The 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; required use of information sharing systems 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.

f. 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, NRC reviews of site security plans, implementation of the enhanced baseline inspection program and evaluations of force-on-force exercises. These new requirements include additional physical 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, qualification requirements for security trainers, armorer certification requirements, program requirements for on-the-job training, and qualification requirements for drill and exercise controllers.

g. Physical security enhancements. The rule imposes new physical security enhancements in the revised section 73.55 that were identified by the NRC 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 section 73.55 include a requirement that the central alarm station (CAS) and secondary alarm station (SAS) have functionally equivalent capabilities such that no single act in accordance with the design basis threat of radiological sabotage can 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 section 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.

Significant Changes in the Final Rule

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

a. Bifurcation of Enhanced Weapons Requirements. As discussed above, section 161A. of the AEA permits the NRC to authorize the use of certain enhanced weapons in the protective strategies of specific designated licensees once guidelines are developed by the NRC and approved by the Attorney General (from section 653 of EPAct 2005). In anticipation of the completion of those guidelines, the proposed rule contained several provisions that would have described the requirements for the use of enhanced weapons and for firearms background checks for certain security personnel (i.e., proposed § 73.18 and § 73.19). Since the guidelines have not yet received the approval of the Attorney General, the NRC decided to separate that portion of the proposed rule to be continued as a separate rulemaking, accordingly this final rule does not contain any provisions related to the implementation of Section 161A.

b. Cyber Security Requirements. Another change to this final rulemaking is the re-location of cyber security requirements. Cyber security requirements had been located in the proposed rule in paragraph 73.55(m). These requirements are now placed into new section 73.54 as a separate section within part 73. 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. Establishing these requirements as a stand-alone section also necessitated creating accompanying licensing requirements. Since 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 separated, the NRC 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 above and in section 73.54, for current reactor licensees, the rule requires the submission a new cyber security plan to the NRC for review and approval within 180 days of the effective date of the 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 operating license who have submitted their applications to the NRC 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.

c. Performance Evaluation. 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.

d. Mitigative strategies and response procedures for potential or actual aircraft attacks. Another significant change to this rulemaking is the re-location 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 since the requirements were not specific to the licensee's security organization. The NRC agreed and relocated the requirements accordingly, and provide more details to the rule language to ensure that the intent of these requirements was clear. As noted above, the NRC issued a supplemental proposed rule seeking additional stakeholder comment on these proposed changes to the rule.

e. Section 73.71 and Appendix G. The proposed power reactor security rulemaking contained proposed requirements for section 73.71 and appendix G to part 73. The Commission intended to make few changes to these regulations based on public comments. However, these provisions are not contained in this final rulemaking. Because the enhanced

weapons rulemaking will include potential changes to section 73.71 and appendix G, the Commission decided that revisions to these regulations were better suited for that rulemaking.

f. 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 submit these security plans for NRC review and approval. The final rule no longer requires these security plans (with the exception of the cyber security plan as discussed above) to be submitted for prior NRC 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 since most of the requirements established by this rule are substantially similar to the requirements that had been imposed by the security orders, and all licensee security plans were recently reviewed and approved by the NRC in 2004 following issuance of the 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 NRC. For the requirements that go beyond current practices, the Commission does not expect that changes that would be required by this rule would result in decreases of effectiveness in 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 NRC 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 operating license as for 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.

g. EPAct of 2005 Provisions. The proposed rule contained a number of proposed requirements that were designed to address security-related provisions of the EPAct of 2005. With respect to Section 653 of the EPAct of 2005, the enhanced weapons and firearms background check requirements have been moved to a separate rulemaking. The only other provisions of the EPAct of 2005 that the NRC had considered during this rulemaking were in Section 651, which concerns matters related to the triennial NRC-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 of 2005, and has submitted three annual reports to Congress during that time.

h. 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 concluded that these terms are better addressed in guidance, and accordingly the final rule does not contain these provisions.

Conforming Changes

Conforming changes to the requirements listed below are made to 1) ensure that cross-referencing between the various security regulations in part 73 is preserved, 2) implement cyber security plan submittal requirements, and 3) preserve requirements for licensees who are not within the scope of this rule. The following requirements contain conforming changes:

- Section 50.34, “Contents of construction permits and operating license applications; technical information” is revised to align the application requirements with the revisions to appendix B to 10 CFR part 73, the addition of section § 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 paragraph to section 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 section § 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 since willful violations of the new §§ 73.54 and 73.58 may be subject to criminal sanctions.

Appendix B and appendix C to part 73 require special treatment in this rulemaking to preserve, with a minimum of conforming changes, the current requirements for licensees and

applicants who are not within the scope of this rule. Accordingly, sections I through V of part 73 appendix B 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 rulemaking, and the new language for power reactor security training and qualification (revised in this rulemaking) 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 rule such as Category I strategic special nuclear material licensees and research and test reactor licensees), and section II containing all new requirements related to power reactor contingency response.

ENVIRONMENTAL ASSESSMENT

Identification of the Action:

1) Make generically applicable security requirements similar to those previously imposed by Commission orders issued after the terrorist attacks of September 11, 2001, based upon experience and insights gained by the Commission during implementation of those orders;
2) Add several new requirements that resulted from insights from implementation of the security orders, review of site security plans, and implementation of the enhanced baseline inspection program and force-on-force exercises;
3) Update the regulatory framework in preparation for receiving license applications for new reactors; and,
4) Consider the issues raised in three petitions for rulemaking (consistent with the petition closure and resolution process) during the development of the final rule requirements.

The Need for the Action:

The action is principally needed because the NRC has determined that the security requirements similar to those previously imposed by orders following the attacks of September 11, 2001, and which applied only to existing licensees, should be made generically applicable to all power reactor applicants and future licensees. The requirements of this rulemaking represent the NRC's view on the security requirements that are necessary for the adequate protection of the public health and safety and the common defense and security, or have been determined to be substantial security enhancements. In addition, the NRC is taking this action to accomplish the other stated objectives above.

Environmental Impacts of the Proposed Action:

This environmental assessment focuses on those aspects of the power reactor security rulemaking where there is a potential for the revised requirements to affect the environment. The NRC has concluded that there will be no significant radiological environmental impacts associated with implementation of the final power reactor security rule requirements for the following reasons:

(1) The revision to the power reactor security requirements does not result in changes to the design basis requirements for the structures, systems, and components (SSCs) in affected licensees' facilities that function to limit the release of radiological effluents during and following postulated accidents. All the SSCs associated with limiting the releases of offsite radiological effluents will therefore continue to be able to perform their functions, and as a result, there is no significant radiological effluent impact. The NRC also notes that the safety-security interface requirements (new section § 73.58) are added to Part 73 to explicitly require, what was previously implicitly required by the regulations, that plant activities should not adversely 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 NRC expects that § 73.58 will enhance safety and security.

(2) The standards and requirements applicable to radiological releases and effluents are not affected by the power reactor security rulemaking and continue to apply to the SSCs affected by the power reactor security rulemaking.

The principal effect of this action is to revise the governing regulations pertaining to power reactor security, make generically applicable security requirements similar to those previously imposed post 9/11 orders, and to add additional requirements consistent with the rulemaking objectives discussed earlier. None of the revisions affect current occupational exposure requirements, consequently the NRC has concluded that this action has no impact on occupational exposure.

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

With regard to potential non-radiological impacts, implementation of the rule requirements does not have a significant impact on the environment. Though the requirements of this rule may result in some licensees to make modifications at their facilities, the NRC does not anticipate such modifications to have any significant environmental impact. In addition, the revised requirements 1) do not affect any historic sites, and 2) do not affect non-radiological plant effluents. Therefore, there is no significant non-radiological environmental impact associated with this final rule action.

Accordingly, the NRC concludes that there is no significant environmental impact associated with the final rulemaking action.

Alternatives to the Proposed Action:

As an alternative to the rulemakings described above, the NRC staff considered not taking the action (i.e., the "no-action" alternative). Not revising the security regulations results in no change in current environmental impacts since the requirements would result in no significant environmental impact. Therefore, taking no action results in no net change to the environmental impact. However, the no action alternative would leave the existing security requirements intact, and as such, the NRC's security requirements for nuclear power plants would not reflect the requirements that the NRC has concluded are necessary for the adequate protection of the public health and safety and the common defense and security. This "no action" would not only affect the security at currently operating reactors, but would also hinder the NRC's ability to impose adequate security measures on future nuclear power plants. Failure to codify these security requirements would also significantly impact the NRC's statutory obligation under the Atomic Energy Act of 1954, as amended, (AEA) to establish rules or regulations that are necessary to provide for the adequate protection of the health and safety of the public and be in accord with the common defense and security.

Alternative Use of Resources:

This action does not involve the use of any resources not previously considered by the NRC in its past environmental statements for issuance of operating licenses for the facilities that are affected by this action.

Agencies and Persons Consulted:

The NRC staff developed the rule and this environmental assessment. The NRC provided state liaison officials with a copy of the proposed rule and requested comment. No comments were received on the environmental assessment. No other agencies were consulted.

FINDING OF NO SIGNIFICANT IMPACT

On the basis of the environmental assessment, the NRC concludes that the action will not result in a significant effect on the quality of the human environment. Accordingly, the NRC did not prepare an environmental impact statement for the action.

Documents may be examined and/or copied for a fee, at the NRC's Public Document Room, located at One White Flint North, 11555 Rockville Pike (first floor), Rockville, Maryland 20852. Publicly available records will be accessible electronically from the Agencywide Documents Access and Management System (ADAMS) Public Library component on the NRC web site http://www.nrc.gov (Electronic Reading Room).

Dated at Rockville, Maryland, this th day of , 2008.

FOR THE NUCLEAR REGULATORY COMMISSION

Michael J. Case, Director
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation