[7590-01-P]

NUCLEAR REGULATORY COMMISSION

10 CFR Parts 50, 72, and 73

RIN 3150-AG63

Power Reactor Security Requirements

AGENCY: Nuclear Regulatory Commission.

ACTION: Proposed rule.

SUMMARY: The Nuclear Regulatory Commission (NRC) is proposing to amend the current security regulations and add new security requirements pertaining to nuclear power reactors. Additionally, this rulemaking includes new security requirements for Category I strategic special nuclear material (SSNM) facilities for access to enhanced weapons and firearms background checks. The proposed rulemaking would: make generically applicable security requirements imposed by Commission orders issued after the terrorist attacks of September 11, 2001, based upon experience and insights gained by the Commission during implementation; fulfill certain provisions of the Energy Policy Act of 2005; 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 impose requirements to assess and manage site activities that can adversely affect safety and security. The proposed safety and security requirements would address, in part, a petition for rulemaking (PRM 50-80) that requests the establishment of regulations

governing proposed changes to facilities which could adversely affect the protection against radiological sabotage.

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

ADDRESSES: You may submit comments by any one of the following methods. Please include the following number “RIN 3150-AG63" in the subject line of your comments. Comments on rulemakings submitted in writing or in electronic form will be made available for public inspection. Because your comments will not be edited to remove any identifying or contact information, the NRC cautions you against including any information in your submission that you do not want to be publicly disclosed.

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

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

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

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

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

Publicly available documents related to this rulemaking may be viewed electronically on the public computers located at the NRC's Public Document Room (PDR), O1-F21, One White Flint North, 11555 Rockville Pike, Rockville, MD 20852-2738. The PDR reproduction contractor will copy documents for a fee. Selected documents, including comments, may be viewed and downloaded electronically via the NRC rulemaking web site at http://ruleforum.llnl.gov.

Publicly available documents created or received at the NRC after November 1, 1999, are available electronically at the NRC's Electronic Reading Room at http://www.nrc.gov/reading-rm/adams.html. From this site, the public can gain entry into the NRC's Agencywide Document Access and Management System (ADAMS), which provides text and image files of 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 PDR Reference staff at 1-800-397-4209, 301-415-4737, or by e-mail to PDR@nrc.gov.

FOR FURTHER INFORMATION CONTACT: Mr. Richard Rasmussen, Office of Nuclear Security and Incident Response, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001; telephone (301) 415-0610; e-mail: RAR@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: TAR@nrc.gov.

SUPPLEMENTARY INFORMATION

Table of Contents

I. Background.

II. Rulemaking Initiation.

III. Proposed Regulations.

IV. Section-by-Section Analysis.

V. Guidance.

VI. Criminal Penalties.

VII. Compatibility of Agreement State Regulations.

VIII. Availability of Documents.

IX. Plain Language.

X. Voluntary Consensus Standards.

XI. Finding of No Significant Environmental Impact.

XII. Paperwork Reduction Act Statement.

XIII. Public Protection Notification.

XIV. Regulatory Analysis.

XV. Regulatory Flexibility Certification.

XVI. Backfit Analysis.

I. Background

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 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.

Most of the requirements in this proposed rulemaking are derived directly from, or through implementation of, the following four security orders:

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

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. These plans incorporated the enhancements instituted through the orders. While the specifics of these changes are Safeguards Information, 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 Energy Policy Act of 2005 (EPAct 2005), signed into law on August 8, 2005, is another source of some of the proposed requirements reflected in this rulemaking. Section 653, for instance, allows the NRC to authorize 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 that all security personnel with access to any weapons undergo a background check that would include fingerprinting and a check against the Federal Bureau of Investigation's (FBI) National Instant Criminal Background Check System (NICS) database. These provisions of EPAct 2005 would be reflected in the newly proposed §§ 73.18 and 73.19, and the proposed NRC Form 754. Though this rulemaking primarily affects power reactor security requirements, to implement the EPAct 2005 provisions efficiently, the NRC expanded the rulemaking's scope in newly proposed §§ 73.18 and 73.19 to include facilities authorized to possess formula quantities or greater of strategic special nuclear material, i.e., Category I SSNM facilities. Such facilities would include production facilities, spent fuel reprocessing facilities, fuel processing facilities, and uranium enrichment facilities. Additionally, Section 651 of the EPAct 2005 requires the NRC to conduct security evaluations at selected licensed facilities, including periodic force-on-force exercises. That provision also requires the NRC to mitigate any potential conflict of interest that could influence the results of force-on-force exercises. These provisions would be reflected in proposed § 73.55.

Through 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, the NRC has identified some additional security measures that would provide additional assurance of a licensee's capability to protect against the DBT.

Finally, a petition for rulemaking submitted by the Union of Concerned Scientists and San Luis Obispo Mothers for Peace (PRM 50-80), requested the establishment of regulations governing proposed changes to facilities which could adversely affect their protection against radiological sabotage. This petition was partially granted on November 17, 2005 (70 FR 69690). The proposed new § 73.58 contains requirements to address te remaining issues.

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

- 10 CFR 73.2, Definitions.
- 10 CFR 73.55, Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.
- 10 CFR 73.56, Personnel access authorization requirements for nuclear power plants.
- 10 CFR 73.71, Reporting of safeguards events.
- 10 CFR 73, Appendix B, General criteria for security personnel.
- 10 CFR 73, Appendix C, Licensee safeguards contingency plans.
- 10 CFR 73, Appendix G, Reportable safeguards events.

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

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

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

<u>EPAct 2005 weapons guidelines</u>

In order to accomplish Sec. 161A. of the Atomic Energy Act of 1954, as amended (AEA), concerning the transfer, receipt, possession, transport, import, and use of enhanced weapons and the requirements for firearms background checks, the NRC has engaged with representatives from the U.S. Department of Justice (DOJ), the FBI, and the U.S. Bureau of

Alcohol, Tobacco, Firearms, and Explosives (ATF), to develop guidelines required by Sec. 161A.d of the AEA. The provisions of Sec.161A. of the AEA take affect upon the issuance of these guidelines by the Commission, with the approval of the Attorney General. The Commission will publish a separate *Federal Register* notice on the issuance of these guidelines. This proposed rule would not rescind the authority of certain NRC licensees, currently possessing automatic weapons through alternate processes, to possess such enhanced weapons; however, these licensees would be subject to the new firearms background check requirements of Sec.161A. of the AEA. Information on new provisions (§§ 73.18 and 73.19) that would implement Sec. 161A. may be found in Section III.

Conforming and Corrective Changes

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

- Section 50.34, “Contents of applications; technical information” would be revised to align the application requirements with the proposed revisions to appendix C to 10 CFR Part 73.
- Section 50.54, “Conditions of licenses” would be revised to conform with the proposed revisions to sections in appendix C to 10 CFR part 73.
- Section 50.72, "Immediate notification requirements for operating nuclear power reactors" would be revised to state (in footnote 1) that immediate notification to the NRC may be required (per the proposed § 73.71 requirements) prior to the notification requirements under the current § 50.72.

- Section 72.212, “Conditions of general license issued under § 72.210” would be revised to reference the appropriate revised paragraph designations in proposed § 73.55.
- Section 73.8, “Information collection requirements: OMB approval” would be revised to add the newly proposed requirements (§§ 73.18, 73.19, 73.58, and NRC Form 754) to the list of sections and forms with Office of Management and Budget (OMB) information collection requirements. A corrective revision to § 73.8 would also be made to reflect OMB approval of existing information collection requirements for NRC Form 366 under existing § 73.71.
- Section 73.70, “Records” would be revised to reference the appropriate revised paragraph designations in proposed § 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 newly proposed §§ 73.18, 73.19, and 73.58 may be subject to criminal sanctions.

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

II. Rulemaking Initiation

On July 19, 2004, NRC staff issued a memorandum entitled “Status of Security-Related Rulemaking” (accession number ML041180532) to inform the Commission of plans to close former security-related actions and replace them with a comprehensive rulemaking plan to modify physical protection requirements for power reactors. This memorandum described rulemaking efforts that were suspended by the terrorist activities of September 11, 2001, and summarized the security-related actions taken following the attack. In response to this memorandum, the Commission directed the staff in an August 23, 2004, Staff Requirements Memorandum (SRM) (COMSECY-04-0047, accession number ML042360548) to forego the development of a rulemaking plan, and provide a schedule for the completion of security-related rulemakings. The staff provided this schedule to the Commission by memorandum dated November 16, 2004 (accession number ML043060572). Subsequently, the staff revised its plans to amend the part 73 security requirements to include a requirement for licensees to assess and manage site activities that could compromise either safety or security (i.e., the safety/security interface requirements). This revision is discussed in a memorandum dated July 29, 2005 (accession number ML051800350). Finally, by memorandum dated September 29, 2005 (COMSECY-05-0046, accession number ML052710167), the staff discussed its plans to incorporate select provisions of the EPAct 2005 into the power reactor security requirements rulemaking. In COMSECY-05-0046, dated November 1, 2005 (accession number ML053050439), the Commission-approved the staff’s approach in incorporating the select provisions of EPAct 2005.

III. Proposed Regulations

This section describes significant provisions of this rulemaking:

1. EPAct 2005 weapons requirements. The new §§ 73.18 and 73.19 would contain requirements to implement provisions of section 161A of the Atomic Energy Act of 1954, as amended (AEA). Section 653 of the EPAct amended the AEA by adding section 161A, "Use of Firearms by Security Personnel." Section 161A provides new authority to the Commission to enhance security at certain NRC licensee and certificate holder facilities by authorizing the security personnel of those licensees or certificate holders to transfer, receive, possess, transport, import, and use an expanded arsenal of weapons, to include: short-barreled shotguns, short-barreled rifles, and machine guns. In addition, section 161A also provides that NRC-designated licensees and certificate holders may apply to the NRC for authority to preempt local, State, or certain Federal firearms laws (including regulations) that prohibits the transfer, receipt, possession, transportation, importation, or use of handguns, rifles, shotguns, short-barreled shotguns, short-barreled rifles, machineguns, semiautomatic assault weapons, ammunition for such guns or weapons, and large capacity ammunition feeding devices. Prior to granting either authority, however, the Commission must determine that the proposed use of this authority is necessary in the discharge of official duties by security personnel engaged in protecting: (1) facilities owned or operated by an NRC licensee or certificate holder and designated by the Commission, or (2) radioactive material or other property that is owned or possessed by an NRC licensee or certificate holder, or that is being transported to or from an NRC-regulated facility, if the Commission has determined the radioactive material or other property to be of significance to the common

defense and security or public health and safety. Licensees and certificate holders must receive preemption authority before receiving NRC approval for enhanced weapons authority. Finally, the NRC may consider making preemption authority or enhanced-weapons authority available to other types of licensees or certificate holders in future rulemakings.

Under the provisions of section 161A.d, section 161A takes effect on the date that implementing guidelines are issued by the Commission after being approved by the U.S. Attorney General. Following enactment of the EPAct 2005, NRC staff began discussions with staffs from the U.S. Department of Justice (DOJ) and its subordinate agencies the Federal Bureau of Investigation (FBI) and the U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) to develop these guidelines. Issuance of these guidelines is a prerequisite for the issuance of a final rule on §§ 73.18 and 73.19, and the conforming changes in § 73.2. The proposed language for §§ 73.18 and 73.19, and the conforming changes in § 73.2, set forth in this proposed rule is consistent, to the extent possible, with the discussions between NRC and DOJ. However, because NRC and DOJ staffs continue to work to resolve the remaining issues, the guidelines have not been finalized as of the issuance of this notice. Once the final guidelines are issued, the Commission will, if necessary, take the appropriate actions to ensure that the language of proposed §§ 73.18, 73.19, and 73.2, conforms with the guidelines. The Commission is utilizing this parallel approach to provide the most expeditious process for promulgating the necessary regulations implementing section 161A; thereby enhancing the security (i.e., weapons) capabilities of NRC-licensed facilities, while being mindful of our obligations to provide stakeholders an opportunity to comment on proposed regulations.

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

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

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

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

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

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

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

implemented under the circumstances associated with the loss of large areas of the plant due to explosions or fire. These proposed requirements would be incorporated into the proposed appendix C to part 73.

8. Access authorization enhancements. The proposed changes would improve the integration of the access authorization requirements, fitness-for-duty requirements, and security program requirements. The proposed rule would include an increase in the rigor for some elements of the access authorization program including requirements for the conduct of psychological assessments, requirements for individuals to report arrests to the reviewing official, and requirements to clarify the responsibility for the acceptance of shared information. The proposed rule would also add requirements to allow NRC inspection of licensee information sharing records and 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.

9. Training and qualification enhancements. The proposed rule includes modifications to the training and qualification requirements that are based on 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 new requirements would include additional physical requirements for unarmed security personnel to assure that personnel performing these functions meet physical requirements commensurate with their duties. Proposed new requirements also include a minimum age requirement of

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

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

11. Miscellaneous. The proposed rule would eliminate some requirements that the staff found to be unnecessary, while still providing 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. One such requirement to be eliminated provides for guards to escort operators of motor vehicles within the protected area if the operators are cleared

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

IV. Section-by-Section Analysis

IV.1. New weapons requirements.

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

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

Under proposed § 73.18, after the NRC approves the licensee’s or certificate holder’s application, all security personnel must have a satisfactorily completed firearms background check to have access to covered weapons. Licensees and certificate holders would be required under proposed § 73.19 to notify the NRC that they have satisfactorily completed a sufficient number of firearms background checks to staff their security organization. The

firearms background checks required by proposed § 73.18 would be intended to verify that armed security personnel are not prohibited from receiving, possessing, transporting, or using firearms under Federal or State law. A firearms background check would consist of two parts, a check of an individual's fingerprints against the FBI's fingerprint system and a check of the individual's identity against the FBI's National Instant Criminal Background Check System (NICS). The NRC would propose a new NRC Form 754 for licensee or certificate holder security personnel to submit the necessary information to the NRC for forwarding to the FBI to perform the NICS portion of the firearms background check. The requirement to satisfactorily complete a firearms background check would apply to security personnel either directly employed by the licensee or certificate holder or employed by a security contractor to the licensee or certificate holder and whose official duties require access to covered weapons (i.e., armed security personnel) [see also new definitions for *covered weapons*, *enhanced weapons*, and *standard weapons* in § 73.2]. Additionally, the requirement for licensees or certificate holders to ensure that their security personnel have satisfactorily completed a firearms background check would apply to licensees and certificate holders who have applied for and received NRC approval of preemption authority or enhanced-weapons authority. In order to simplify the rule language, § 73.18 would only refer to applications for preemption authority because preemption authority would always be a necessary prerequisite for the receipt of enhanced weapons authority.

The NRC would propose that a licensee or certificate holder may begin firearms background checks on armed security personnel after the licensee or certificate holder has applied to the NRC for the preemption authority section 161A of the AEA. Because the NRC has not previously had the authority to require its licensees or certificate holders to complete firearms background checks on security personnel, in most instances these requirements would be new to licensees and uncertainties exist over the amount of time to complete these checks.

Thus delays in completing the checks (e.g., the time necessary to resolve any errors of fact in the FBI's NICS databases) could reduce the number of available security officers and create fatigue or minimum staffing level issues. Therefore, the NRC envisions working with licensees and certificate holders on a case-by-case basis to establish the date for NRC approval of an application for preemption authority; and thereby ensure that the licensee's or certificate holder's security organizations can continue to adequately protect the facility when the approval is issued.

The Commission has not yet determined whether licensees and certificate holders may apply for preemption authority alone or combined preemption and enhanced-weapons authority prior to issuance of a final rule. In anticipation that the Commission does permit applications for section 161A authority prior to promulgation of a final rule, the proposed rule would include language to support a transition to these regulations from requirements imposed by Commission orders granting section 161A authority. The proposed rule would not; however, require a licensee or certificate holder to repeat a firearms background check for security personnel who previously satisfactorily completed a firearms background check that was required under Commission order. Consequently, this approach would provide both the Commission and industry with the maximum flexibility to expeditiously implement the security enhancements authorized by section 161A. The exception to this requirement would be for security personnel who have had a break in employment with the licensee or certificate holder or their security contractor, or who have transferred from another licensee or certificate holder (who previously completed a firearms background check on them). In either case these security personnel would be treated as new security personnel and they would be subject to a new firearms background check.

The proposed rule would also provide direction on how security personnel who have received an adverse firearms background check (i.e., a "denied" or "delayed" NICS response)

may: 1) obtain further information from the FBI on the reason for the adverse response, 2) appeal a “denied” response, or 3) provide additional information to resolve a “delayed” response. Security personnel would be required to apply directly to the FBI for these actions (i.e., the licensee or certificate holder may not appeal to the FBI on behalf of the security personnel). Only after such personnel have successfully appealed their “denied” response, and have subsequently received a “proceed” NICS response, would they be permitted access to covered weapons.

Security personnel who receive a “denied” NICS response are presumed by ATF to be prohibited from possessing or receiving a firearm under federal law (see 18 U.S.C. 922) and may not have access to covered weapons unless they have successfully appealed the “denied” NICS response and received a “proceed” NICS response. Because of the structure of section 161A, the proposed rule would not require licensees or certificate holders to remove personnel with a “denied” response until after the NRC has approved the licensee’s or certificate holder’s application for preemption authority (i.e., licensee’s and certificate holders would not be subject to the requirements of § 73.18 until after the NRC’s approval of their application for preemption authority is issued). However, the NRC’s expectation is that current licensees or certificate holders who receive a “denied” response for current security personnel would remove those personnel from any security duties requiring possession of firearms to comport with applicable Federal law and ATF regulations.

The NRC would propose to charge the same fee for fingerprints submitted for a firearms background check as is currently imposed for fingerprints submitted for other NRC-required criminal history checks including fingerprints (i.e., an NRC administrative fee plus the FBI’s processing fee). In addition, the NRC would charge an administrative fee for processing the NICS check information, however, no FBI fee would be charged for the NICS check.

The proposed § 73.19 would only apply to power reactor licensees and Category I special nuclear material licensees; therefore, only these two classes of licensees would be subject to the firearms background check provisions of § 73.18. The NRC may, however, consider making stand-alone preemption authority or combined enhanced-weapons authority and preemption authority available to other types of licensees or certificate holders in future rulemakings.

In § 73.19, the NRC would propose requirements for a licensee or certificate holder to apply for stand-alone preemption authority or to apply for combined enhanced-weapons authority and preemption authority. Licensees and certificate holders who apply for enhanced-weapons authority, must also apply for and receive NRC approval of preemption authority as a necessary prerequisite to receiving enhanced-weapons authority. The NRC would propose limiting either authority to power reactor licensees and Category I SSNM licensees at this time. The NRC may consider applying this authority to other types of licensees, certificate holders, radioactive material, or other property (as authorized under section 161A) in future rulemakings. Obtaining enhanced-weapons authority from the NRC would be a necessary prerequisite for a licensee or certificate holder to apply under ATF's regulations for a Federal firearms license for these weapons. The NRC would propose that licensees and certificate holders who want to apply for enhanced-weapons authority must provide the NRC, for prior review and approval, a new or revised security plan, training and qualification plan, and safeguards contingency plan to reflect the use of these specific new weapons the licensee or certificate holder intends to employ and to provide a safety assessment of the onsite and offsite impact of these specific enhanced weapons.

The proposed rule would also provide direction on acceptable training standards for training and qualification on enhanced weapons. The NRC would require licensees and certificate holders to complete training and qualification of security personnel on any enhanced

weapons, before these personnel employ those weapons to protect the facility. The NRC would also require Commission licensees and certificate holders to notify the NRC of any adverse ATF findings associated with ATF's inspections, audits, or reviews of their Federal firearms license (FFL) (i.e., an FFL held by an NRC licencee or certificate holder).

Finally, the NRC would propose to treat enhanced weapons the same as existing weapons for the purpose of "use" of these weapons; and therefore § 73.19 would cross reference to existing regulation in §§ 73.55 and 73.46 on the use of weapons by reactor licensees and by Category I SSNM licensees (i.e., the NRC is not proposing separate requirements on enhanced weapons versus standard weapons; rather, requirements on the use of any weaponry possessed by the licensee or certificate holder should be appropriate for the facility).

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

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

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

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

govern power reactor security programs. The remaining paragraphs of § 73.55 would implement the detailed requirements for each of the security plans, as well as for the various features of physical security.

This section would be extensively revised in an effort to make generically applicable security requirements imposed by Commission orders issued after the terrorist attacks of September 11, 2001, based upon experience and insights gained by the Commission during implementation, fulfill certain provisions of the EPAct of 2005, and add several new requirements that resulted from evaluation insights from implementation of the security orders, review of site security plans, and implementation of the enhanced baseline inspection program and force-on-force exercises. The proposed regulations would require an integrated security plan that begins at the owner controlled area boundary and would implement defense-in-depth concepts and protective strategies based on protecting target sets from the various attributes of the design basis threat. Notable additions to the proposed § 73.55 are summarized below.

Cyber Security Requirements

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

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

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

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

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

The NRC has concluded that protecting the alarm stations such that a single act does not disable the key functions would provide an enhanced level of assurance that a licensee can

maintain detection, assessment and communications capabilities required to protect the facility against the design basis threat of radiological sabotage. For new reactor licensees, licensed after the publication of this rule, the Commission would require CAS and SAS to be designed, constructed, and equipped with equivalent standards.

Uninterruptible Power for Intrusion Detection and Assessment Systems

Current regulatory requirements require back-up power for alarm annunciation and non-portable communication equipment, but do not require this back-up power to be uninterruptible. Although not specifically required, many licensees have installed uninterruptible power to their security systems for added reliability of these electronic systems. However, the Commission had not required uninterruptible power for assessment systems. For the purposes of assessing the regulatory burden of this proposed rule, the NRC assumed that only a small number of licensees would require hardware modifications to meet this proposed requirement.

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

"Video-Capture" Capability

Current regulatory requirements address the use of closed circuit television systems, but do not explicitly require them. Although not specifically required, all licensees have adopted the use of video surveillance in their site security plans. Many of the licensees have adopted advanced video surveillance technology to provide real-time and play-back/recorded video images to assist security personnel in determining the cause of an alarm annunciation. For the

purposes of assessing the regulatory burden of this proposed rule, the NRC assumed that a small percentage of licensees would require hardware modifications to comply with this proposed requirement for advanced video surveillance technology.

Through implementation of the Commission-approved security plans, baseline inspections, and force-on-force testing, the NRC has concluded that advanced video technology would provide an enhanced level of assurance that a licensee can assess the cause of an alarm annunciation and initiate a timely response capable of defending the facility against the threat up to and including the design basis threat of radiological sabotage. Therefore the proposed rule would require advanced video surveillance technology.

Implementation of § 73.55 is linked principally to the application of appendix B to part 73, "General criteria for security personnel," and appendix C to part 73, "Licensee safeguards contingency plans," both of which would be revised in this proposed rulemaking. Proposed changes to these appendices are discussed in Sections IV.6 and IV.7 of this document.

Table 2 sets forth the proposed § 73.55 language as compared to the current language, and provides the supporting discussion for the proposed language including new definitions for *security officer* and *target set* that would be added to § 73.2. Because § 73.55 would be restructured extensively, Table 9 (See Section VIII) provides a cross reference to locate individual requirements of the current regulation within the proposed regulation.

The Commission is interested in obtaining specific stakeholder input on the impacts and burdens for certain areas of proposed changes to § 73.55. Due to the accelerated rulemaking schedule, the NRC staff's assessments of impacts to individual licensees as a result of the proposed new requirements have not been informed by stakeholder insights on potential implementation issues. Consequently, the Commission recognizes that its views on the feasability, costs, and time necessary to fully implement certain portions of this proposed rule (e.g., alarm station, supporting systems, video systems, and cyber security issues) by selected

licensees may not be fully informed. Accordingly, the Commission is requesting persons commenting on this proposed rule to address the following questions:

1. What insights and estimates can stakeholders provide on the feasability, costs, and time necessary to implement the proposed rule's changes to existing alarm stations, supporting systems, video systems, and cyber security?
2. Are there any actions that should be considered, such as authorizing alternative measures, exemptions, extended implementation schedules, etc., that would allow the NRC to mitigate any unnecessary regulatory burden created by these requirements?

IV.3. Section 73.56, "Personnel access authorization requirements for nuclear power plants."

This section would continue to apply to all current Part 50 licensees and to all applicants who are applying for a new reactor license under Parts 50 or 52, but would be extensively revised. Proposed § 73.56 would retain the requirement for a licensee to determine that an individual is trustworthy and reliable before permitting the individual to have unescorted access to nuclear power plant protected areas and vital areas. The majority of the revisions in proposed § 73.56 reflect several fundamental changes to the NRC's approach to access authorization requirements since the terrorist attacks of September 11, 2001, and the NRC's concern with the threat of an active or passive insider who may collude with adversaries to commit radiological sabotage. These changes would include: 1) an increase in the rigor of some elements of the access authorization program to provide increased assurance that individuals who have unescorted access authorization are trustworthy and reliable; 2) an elimination of temporary unescorted access provisions [prior to the completion of the full background check]; 3) an elimination of the provisions that permit relaxation of the program

when a reactor is in cold shutdown; and 4) the addition of a new category of individuals who would be subject to § 73.56.

Proposed § 73.56(b)(ii) would require licensees' 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 computer technology to maximize plant productivity. In general, licensees currently exclude from their access authorization programs, individuals who may electronically access equipment in the protected areas of nuclear power plants to perform their job functions, if their duties and responsibilities do not require physical unescorted access to the equipment located within protected or vital areas. However, because these individuals manage and maintain the networks that connect to equipment located within protected or vital areas and are responsible for permitting authorized and/or trusted personnel to gain electronic access to equipment and systems, they are often granted greater electronic privileges than the trusted and authorized personnel. With advancements in electronic technology and telecommunications, differences in the potential adverse impacts of a saboteur's actions through physical access and electronic access are lessening. Thus, the proposed rule would require those individuals who have authority to electronically access equipment that, if compromised, can adversely impact operational safety, security or emergency preparedness of the nuclear power plants, to be determined to be trustworthy and reliable.

The proposed revisions to § 73.56 would also address changes in the nuclear industry's structure and business practices since this rule was originally promulgated. At the time the current § 73.56 was developed, personnel transfers between licensees (i.e., leaving the

employment of one licensee to work for another licensee) with interruptions in unescorted access authorization were less common. Most licensees operated plants at a single site and maintained an access authorization program that applied only to that site. When an individual left employment at one site and began working for another licensee, the individual was subject to a different access authorization program that often had different requirements. Because some licensees were reluctant to share information about previous employees with the new employer, licensees often did not have access to the information the previous licensee had gathered about the individual and so were required to gather the necessary information again. The additional effort to collect information that another licensee held created a burden on both licensees and applicants for unescorted access authorization. But, because few individuals transferred, the burden was not excessive.

However, since 1991, the industry has undergone significant consolidation and developed new business practices to use its workforce more efficiently. Industry efforts to better use staffing resources have resulted in the development of a transient workforce that travels from site to site as needed, such as roving outage crews. Although the industry has always relied on contractors and vendors (C/V) for special expertise and staff for outages, the number of transient personnel who work solely in the nuclear industry has increased and the length of time they are on site has decreased. Because the current regulations were written on the basis that the majority of nuclear personnel would remain at one site for years, and that licensees would maintain independent, site-specific access authorization programs and share limited information, the current regulations do not adequately address the transfer of personnel between sites.

In light of the NRC's increased concern with an insider threat since September 11, 2001, the increasingly mobile nuclear industry workforce has heightened the need for information sharing among licensee access authorization programs, including C/V authorization programs

upon which licensees rely, to ensure that licensees have information that is as complete as possible about an individual when making an unescorted access authorization decision. To address this need, the access authorization orders issued by the NRC to nuclear power plant licensees on January 7, 2003, mandated increased sharing of information. In addition, proposed § 73.56 would require licensees and C/V to collect and share greater amounts of information than under the current rule, subject to the protections of individuals' privacy that would be specified in proposed § 73.56(m) [Protection of information]. As a result, individuals who are subject to this section would establish a detailed "track record" within the industry that would potentially cover their activities over long periods of time and would follow them if they change jobs and move to a new position that requires them to be granted unescorted access authorization by another licensee. The proposed requirement acknowledges the industry initiative to develop and utilize a database to ensure accurate information sharing between sites. This increased information sharing is necessary to provide high assurance that individuals who are granted and maintain unescorted access authorization are trustworthy and reliable when individuals move between access authorization programs. In addition, the increased information sharing would reduce regulatory burden on licensees when processing individuals who have had only short breaks between periods of unescorted access authorization.

Another change in the NRC's proposed approach to access authorization requirements is the result of a series of public meetings that were held with stakeholders during 2001–2004 to discuss potential revisions to 10 CFR Part, 26, "Fitness-for-Duty Programs." Part 26 establishes additional steps that the licensees who are subject to § 73.56 must take as part of the process of determining whether to grant unescorted access authorization to an individual or permit an individual to maintain unescorted access authorization. These additional requirements focus on aspects of an individual's behavior, character, and reputation related to

substance abuse. They require the licensee and other entities who are subject to part 26 to conduct drug and alcohol testing of individuals and an inquiry into the individual's past behavior with respect to illegal drug use or consumption of alcohol to excess, as part of determining whether the individual may be granted unescorted access authorization. However, historically there have been some inconsistencies and redundancies between the § 73.56 access authorization requirements and the related requirements in part 26. These inconsistencies have led to implementation questions from licensees, as well as inconsistencies in how licensees have implemented the requirements. The redundancies have, in other cases, imposed an unnecessary regulatory burden on licensees.

During public meetings held to discuss potential changes to part 26, the stakeholders pointed out ambiguities in the terms used in both part 26 and § 73.56, apparent inconsistencies and redundancies in the related requirements, and reported many experiences in which the ambiguities and lack of specificity and clarity in current § 73.56 had resulted in unintended consequences. Although these meetings did not focus on § 73.56, many of the stakeholders' comments directly resulted in some of the proposed changes to § 73.56. (Summaries of these meetings, and any comments provided through the website are available at http://ruleforum.llnl.gov/cgi-bin/rulemake?source=Part26_risk&st=risk.) In response to stakeholder requests, the NRC has proposed language changes to improve the clarity and specificity of the requirements in proposed § 73.56 and substantially reorganized the section to present the requirements generally in the order in which they would apply to licensees' access authorization processes. The proposed changes are expected to result in more uniform implementation of the requirements, and, consequently, greater consistency in achieving the goals of § 73.56. Table 3 sets forth the proposed § 73.56 language as compared to the current language, and discusses the proposed language.

The Commission is interested in obtaining specific stakeholder input on the following two issues:

1. The Commission requests public comment specific to the appropriateness of the framework for the Insider Mitigation Program as specified by the proposed 10 CFR 73.55(b)(7)(i) and 73.55(b)(7)(ii). The proposed rule specifies that the Insider Mitigation Program include elements of the access authorization program, fitness-for-duty program, behavioral observation program, and various physical security measures for the purpose of providing assurance that insider activities would be detected before adverse affects could be realized.

2. The Commission requests public comment on the feasibility of adding a requirement to the proposed rule to require a modified escorted visitor access provision which would allow site visits by members of the public to limited areas of the facility for the purpose of enhancing public education and awareness through informational briefings and tours at the facility.

IV.4. Section 73.58 "Safety/security interface requirements for nuclear power reactors."

The NRC is proposing to add a new requirement to part 73 addressing the safety/security interface for nuclear power reactor licensees. The need for the proposed new requirement is based upon the NRC's experience in reviewing licensees' implementation of a significant number of new security requirements since the terrorist attacks of September 11, 2001. Licensees have always been required to ensure that any changes to safety functions, systems, programs, and activities do not have unintended consequences on other facility safety functions, systems, programs, and activities. Likewise, licensees have been required to ensure that any changes to security functions, systems, programs, and activities do not have

unintended consequences on other facility security functions, systems, programs, and activities. However, the Commission has concluded that the pace, number, and complexity of these security changes warrant the establishment of a more formal program to ensure licensees properly assess the safety/security interface in implementing these changes.

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

The Commission has determined that the proposed safety/security interface rule requirements are necessary because the current regulations do not specifically require evaluation of the effects of plant changes on security or the effects of security changes on plant safety. Further, current regulations do not require communication about the implementation and timing of changes, which would promote awareness of the effects of changing facility conditions and result in appropriate assessment and response.

The NRC is aware of a number of occurrences of adverse safety/security interactions at nuclear power plants over the years to justify consideration of a new rule. Examples of adverse

interactions include: (1) Inadvertent security barrier breaches while performing maintenance activities (e.g., cutting of pipes that provided uncontrolled access to vital areas, removing ventilation fans or other equipment from vital area boundary walls without taking compensatory measures to prevent uncontrolled access into vital areas); (2) Blockage of bullet resisting enclosure's (or other defensive firing position's) fields of fire; (3) Erection of scaffolding and other equipment without due consideration of its impact on the site's applicable physical protection strategy; and (4) Staging of temporary equipment within security isolation zones.

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

The NRC considered many factors in developing this proposed new requirement. One of the factors considered is that existing change processes are focused on specific areas of plant activities, and that implementation of these processes is generally well understood by licensees. An example is found in § 50.54(p), which provides that a reactor licensee may make changes to its safeguards contingency plans without Commission approval provided that the changes do not decrease the safeguards effectiveness of the plan. Similarly, § 50.65(a)(4) provides that a reactor licensee shall assess and manage the increase in risk that may result from proposed maintenance activities. However, neither §§ 50.54(p) (security) nor 50.65(a)(4) (safety) require that an assessment for potential adverse impacts on safety/security interface be made before the proposed changes are implemented. The proposed § 73.58 would address this gap by requiring that, before implementing allowed changes, licensees must assess the

changes with respect to the safety/security interface and, if potential adverse interactions are identified, take appropriate compensatory and/or mitigative action before making the changes.

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

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

IV.5. Section 73.71 “Reporting of safeguards events.”

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

Currently, § 73.71(b)(1) requires power reactor licensees to notify the NRC within one hour of discovery, as described in Paragraph I of appendix G to 10 CFR part 73, "Reportable

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

The proposed amendments to § 73.71 would add a new expedited notification requirement for licensees subject to the provisions of § 73.55 to notify the NRC Operations Center as soon as possible after the discovery of an imminent or actual threat against the facility as described in appendix G to part 73, but not later than 15 minutes after discovery. The proposed amendments to § 73.71 and appendix G to part 73 would also add two additional four-hour notification requirements for suspicious events and tampering events not otherwise covered under appendix G to part 73. The proposed § 73.71 would retain the requirement for the licensee to maintain a continuous communications channel for one-hour notifications upon request of the NRC. The proposed rule would not require a continuous communications channel for four-hour notifications, because of the lesser degree of urgency of these events. For 15-minute notifications, the NRC may request the licensee establish a continuous communications channel after the licensee has made any emergency notifications to State officials or local law enforcement and if the licensee has taken action to stabilize the plant following any transient [associated with the 15-minute notification]. In NRC Bulletin 2005-02,

"Emergency Preparedness and Response Actions for Security-Based Events," dated July 18, 2005, the NRC had indicated a continuous communications channel was not necessary for the new 15-minute notifications. However, in developing this proposed rule the Commission has evaluated the need to promptly obtain information of an unfolding event versus imposing an unreasonable burden on licensees in the midst of a rapidly unfolding event and possible plant transient. The Commission considers that the proposed regulation would provide a reasonable balance between these two objectives. Table 5 sets forth the proposed amendments to § 73.71 language as compared to the current language, and provides the supporting discussion for the proposed language. Table 8 sets forth the proposed amendments to the appendix G to part 73 language as compared to the current language, and provides the supporting discussion for the proposed language.

The Commission is interested in obtaining specific stakeholder input on the proposed changes to § 73.71 and appendix G to part 73 . Accordingly, the Commission is requesting persons commenting on this proposed rule to address the following question:

1. For the types of events covered by the proposed four-hour notification requirements in § 73.71 and appendix G to part 73, should the notification time interval of all or some of these notifications be different (e.g., a 1-hour, 2-hour, 8-hour, 24-hour notification)? If so, what notification time interval is appropriate? "Notification time interval" is meant to be the time from when a licensee recognizes that an event has occurred or is occurring to the time that the licensee reports the event to the NRC.

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

Appendix B to part 73 provides requirements for the training and qualification of security personnel to ensure that security personnel can execute their duties. Following the events of

September 11, 2001, the Commission determined that tactical proficiency and physical fitness requirements governing licensees' armed security force personnel needed to be enhanced. The proposed amendments to appendix B to part 73 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 and add several new requirements that resulted from evaluation insights from force-on-force exercises.

Notable additions to the proposed appendix B to part 73 requirements are summarized as follows:

Additional Physical Requirements and Minimum Age Requirements for Unarmed Members of the Security Organization

Unarmed security personnel perform duties similar to armed security personnel, such as detection, assessment, vehicle and personnel escort, and vital area controls. The current requirements for unarmed members of the security organization 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. The proposed rule would include a requirement to assure that unarmed security personnel are physically capable of performing their assigned duties.

Additionally, the current rule specifies a minimum age of 21 years old for armed security personnel, but does not specify a minimum age requirement for unarmed security personnel. The proposed rule would require that unarmed members attain the age of 18 prior to assignment to establish a minimum age requirement for unarmed members of the security organization at a power reactor facility.

These proposed additional requirements would assure that personnel performing security functions, whether armed or unarmed, meet appropriate age, vision, hearing and psychological requirements commensurate with their assigned security duties.

Qualification Scores for Program Elements Required by the Training and Qualification Plan

The current rule includes daylight qualification scores of 70 percent for handguns, 80 percent for semiautomatic rifles, 50 percent for shotguns and a requirement for night fire familiarization with assigned weapons. The April 29, 2003, Training Order imposed new requirements for the firearms training and qualification programs at power reactor licensees. The Training Order retained the current daylight qualification scores of 70 percent for handguns, 80 percent for semiautomatic rifles and superceded the daylight qualification score of 50 percent for the shotgun. The order did not specify a qualification score for the daylight course of fire for the shotgun, only an acceptable level of proficiency. The order superceded the current rule for night fire familiarization and added courses of fire for night fire and tactical training with assigned weapons.

The proposed rule would retain the qualification scores of the existing regulations and add specific qualification scores for the daylight course of fire for the shotgun and/or enhanced weapons, the night fire qualification for shotguns, handguns, semiautomatic rifles and/or enhanced weapons and the tactical course of fire for all assigned weapons to remain consistent with the qualification scoring methodology contained in the current rule. The scoring methodology for the current rule and the proposed rule is consistent with the scoring methodology used for firearms programs at the local, state and federal levels and is consistent with approved courses of fire from the law enforcement community and recognized national entities.

The proposed rule would also include a requirement for a qualification score of 80 percent for the annual written exam. The current rule does not provide a requirement for an

annual written exam score. Likewise, the April 29, 2003, Training Order that required licensees to develop and implement an annual written exam also did not specify a qualification score. The Commission has determined that a score of 80 percent demonstrates a minimum level of understanding and familiarity of the material necessary to adequately perform security related tasks. The 80 percent score would be consistent with minimum scores commonly utilized throughout the nuclear industry.

Qualification Requirements for Security Trainers, Personnel Assessing Psychological Qualifications and Armorer Certifications

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.

The proposed rule includes specific references to personnel that have assigned duties and responsibilities for implementation of training and qualification programs to ensure these persons are qualified and/or certified to make determinations of security personnel suitability, working condition of security equipment, and overall determinations that security personnel are trained and qualified to execute their assigned duties.

On-the-job Training

The current rule states in part that each individual who requires training to perform assigned security duties shall, prior to assignment, be trained to perform these tasks and duties. Each individual shall demonstrate the required knowledge, skill and ability in accordance with specific standards of each task.

The proposed rule would specify the new requirement that the licensee include on-the-job training as part of the training and qualification program prior to assigning an individual to an unsupervised security position. This requirement is in addition to formal and informal classroom training. The on-the-job training program would provide the licensee 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 proposed revision to appendix B of part 73 required special treatment in this rulemaking to preserve, with a minimum of conforming changes, the current requirements for licensees and applicants to whom this proposed rule would not apply. Accordingly, Section I through V of appendix B to part 73 would remain unchanged, and the proposed new language for power reactors would be added as Section VI.

Table 6 sets forth the proposed amendments to appendix B to part 73 and provides the supporting discussion for the proposed language. Because this section would be extensively restructured, Table 10 (See Section VIII) provides a cross-reference to locate individual requirements of the current regulation within the proposed regulation.

IV.7. Appendix C to Part 73, "Licensee Safeguards Contingency Plans."

Appendix C to part 73 provides requirements that govern the development of safeguards contingency plans. Following the terrorist attacks of September 11, 2001, the NRC conducted a thorough review of security to continue to ensure that nuclear power plants had effective security measures in place given the changing threat environment. The proposed appendix C would increase the information required in the safeguards contingency plans for responses to threats, up to and including, design basis threats, as described in § 73.1. Notable additions to the proposed appendix C to part 73 requirements are summarized below:

<u>Mitigating Strategies</u>

Current regulations do not include requirements to develop mitigating strategies for events beyond the scope of the design basis threat. The orders issued after September 11, 2001, included a requirement to preplan strategies for coping with such events. The proposed appendix C to part 73 would contain this element of the orders to require that licensees preplan

strategies to respond to and mitigate the consequences of potential events, including those that may result in the loss of large areas of the plant due to explosions or fire.

Qualification Requirements for Drill and Exercise Controllers

The current rule and the security orders do not specifically address the qualification of personnel that are assigned duties and responsibilities for implementation of training and qualification drills and exercises at power reactor licensees.

The proposed rule includes specific references to personnel who 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 licensee security force and must be conducted in a manner that demonstrates the licensee's ability to execute the protective strategy as described in the site security plans. Additionally, drills and exercises must be performed properly to assure they do not negatively impact personnel or plant safety.

The proposed revision to appendix C of part 73 required special treatment in this rulemaking to preserve, with a minimum of conforming changes, the current requirements for licensees and applicants to whom this proposed rule would not apply. Accordingly, appendix C to part 73 would be divided into two sections, with Section I maintaining all current requirements, and Section II containing all proposed requirements related to nuclear power reactors.

Table 7 sets forth the proposed amendments to appendix C to part 73 and provides the supporting discussion for the proposed language. Because this section would be extensively restructured, Table 11 (See Section VIII) is a cross-reference showing where individual requirements of the current regulation would be in the proposed regulation.

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

Proposed appendix G to part 73 provides requirements regarding the reporting of safeguards events. Proposed appendix G would contain changes to support the revised and accelerated reporting requirements which would be incorporated into this rulemaking. Proposed appendix G to part 73 would also contain revised four-hour reporting requirements that would require licensees to report to the NRC information of suspicious surveillance activities, attempts at access, or other similar information as addressed in Appendix G, section III (a)(1) and (2). Following September 11, 2001, the NRC issued guidance requesting that licensees report suspicious activities near their facilities to allow assessment by the NRC and other appropriate agencies. The proposed new reporting requirement would clarify this expectation to assure consistent reporting of this important information. Additionally, the proposed rule would contain an additional four-hour reporting requirement for tampering events that do not meet the threshold for reporting under the current one-hour requirements. The proposed reporting requirements for tampering events would allow NRC assessment of these events. Table 8 sets forth the proposed amendments to appendix G to part 73 and provides the supporting discussion for the proposed language.

The Commission is interested in obtaining specific stakeholder input on the following issue:

1. The Commission requests public comment on the need to establish an additional requirement for licensees to establish and maintain predetermined communication protocols, such as passwords, with the Nuclear Regulatory Commission in order to verify the authenticity of communications during a security event, to include requirements for uniform protocols to verify the authenticity of reports required under this proposed rule.

IV.9 Conforming and Corrective Changes.

The following conforming changes would also be made: §§ 50.34 and 50.54 (references to the correct paragraphs of revised appendix C of part 73), § 50.72 (changes to § 73.71 reports), §§ 72.212 and 73.70 (references to the correct paragraphs due to renumbering of § 73.55), and § 73.8 (adding § 73.18, § 73.19, and revised to reflect new NRC form 754 to reflect recordkeeping or reporting burden). A corrective change would also be made to § 73.8 to reflect an existing recordkeeping or reporting burden for NRC Form 366 under § 73.71. However, no changes would be made to § 73.81(b) (due to the new §§ 73.18, 73.19, and 73.58), because willful violations of §§ 73.18, 73.19, and 73.58 may be subject to criminal penalties.

Table 1 - Proposed Part 73.18 and 73.19 and conforming changes to Part 73.2
Firearms background checks for armed security personnel and
authorization for preemption of firearms laws and use of enhanced weapons.

PROPOSED LANGUAGE	CONSIDERATIONS
§ 73.18 **Firearms background checks for armed security personnel.** (a) *Purpose*. This section sets forth the requirements for completion of firearms background checks on armed security personnel at selected NRC-regulated facilities. Firearms background checks are intended to verify that security personnel whose duties require access to covered weapons are not prohibited from receiving, possessing, transporting, importing, or using such weapons under applicable Federal or State law. Licensees and certificate holders listed under paragraph (c) of this section who have applied for preemption authority under § 73.19 (i.e., § 73.19 authority), or who have been granted preemption authority by Commission order, are subject to the requirements of this section.	This new section would implement the firearms background check requirements of new section 161A of the Atomic Energy Act of 1954, as amended. Section 161A was added by section 653 of the Energy Policy Act of 2005. The proposed rule language in §§ 73.18 and 73.19, and conforming changes to § 73.2 would be consistent with the guidelines required by section 161A.d to implement the provisions of section 161A. Section 161A.d requires the Commission to issue guidelines, with the approval of the Attorney General, for section 161A to take effect. In parallel and separate from this rulemaking effort, guidelines are being developed by staffs from the NRC and the Department of Justice (DOJ), [including staffs from the FBI and ATF]. During development of these guidelines, the DOJ indicated that the firearms background check provisions of section 161A only take effect if a triggering event occurs. A triggering event would occur when a licensee or certificate holder applies to the NRC to use the stand-alone preemption authority or the combined enhanced-weapons and preemption authority of section 161A. Therefore, armed security personnel of both current and future licensees and certificate holders would not be subject to the firearms background check provisions of the proposed § 73.18, unless their employing licensee or certificate holder applies for and receives § 73.19 authority from the NRC.

§ 73.18(b) *General Requirements*. (1) Licensees and certificate holders listed in paragraph (c) of this section who have received NRC approval of their application for preemption authority shall ensure that a firearms background check has been satisfactorily completed for all security personnel requiring access to covered weapons as part of their official security duties prior to granting access to any covered weapons to those personnel. Security personnel who have satisfactorily completed a firearms background check, but who have had a break in employment with the licensee, certificate holder, or their security contractor of greater than one (1) week subsequent to their most recent firearms background check, or who have transferred from a different licensee or certificate holder (even though the other licensee or certificate holder satisfactorily completed a firearms background check on such individuals), are not excepted from the requirements of this section.	Paragraph (b)(1) would require current and future licensees and certificate holders who have received NRC approval of their application for preemption authority to ensure that all security personnel whose official duties require access to covered weapons satisfactorily complete a firearms background check. The firearms background check must be satisfactorily completed to permit access to covered weapons. The Commission intends for duties "requiring access to a covered weapon" to include such duties as: security operations activities; training and qualification activities; and weapons' maintenance, handling, accountability, transport, and use activities. [See also new definitions for *covered weapons*, *enhanced weapons*, and *standard weapons* in § 73.2 at the end of Table 1]. A new firearms background check would be required for security personnel who have a break in employment or who have transferred from another licensee or certificate holder irrespective of whether the individual previously satisfactorily completed a firearms background check (i.e., such individuals would be treated as new security personnel and subject to a new firearms background check).

§ 73.18(b)(2) Security personnel who have satisfactorily completed a firearms background check pursuant to Commission orders are not subject to a further firearms background check under this section, unless these personnel have a break in service or transfer as set forth in paragraph (b)(1) of this section.	The NRC staff recognizes that the Commission has not yet made a final decision on whether licensees and certificate holders may apply for preemption authority alone or combined preemption and enhanced-weapons authority prior to issuance of a final rule; however, the proposed rule would include language to support a transfer from any orders associated with such applications for section 161A authority to regulations and thereby provide both the Commission and industry with the maximum flexibility to expeditiously implement the security enhancements of section 161A. Paragraph (b)(2) would exempt previously checked personnel from a recheck, except in the case of a break in service or transfer [as in paragraph (b)(1)].

§ 73.18(b)(3) A change in the licensee, certificate holder, or ownership of a facility, radioactive material, or other property designated under § 73.19, or a change in the security contractor that provides security personnel responsible for protecting such facilities, radioactive material, or other property, shall not constitute ‘a break in service’ or ‘transfer,’ as those terms are used in paragraph (b)(2) of this section. (4) Licensees and certificate holders listed in paragraph (c) of this section may begin the application process for firearms background checks under this section for security personnel whose duties require access to covered weapons immediately on application to the NRC for preemption authority. (5) Firearms background checks do not replace any other background checks or criminal history checks required for the licensee’s or certificate holder’s security personnel under this chapter.	Paragraph (b)(3) would indicate that changes in the security contractor or ownership of the licensee or certificate holder are not triggering events that require a new firearms background check. Paragraph (b)(4) would indicate that Licensee and certificate holders may begin submitting their security personnel for firearms background checks after the licensee or certificate holder has applied to the NRC for preemption authority alone or combined preemption and enhanced weapons authority (i.e., § 73.19 authority). Paragraph (b)(5) would indicate that firearms background checks are in addition to access authorization or security clearance checks that security personnel currently undergo under other NRC regulations (e.g., §§ 11.15, 25.17 or 73.57). The NRC expects licensees and certificate holders who become aware of any new potentially derogatory information on current security personnel (through the completion of a firearms background check), to evaluate any such information for applicability as required by the licensee's or certificate holder's access authorization or security clearance programs.

§ 73.18(c) *Applicability*. This section applies to licensees or certificate holders who have applied for or received NRC approval of their application for § 73.19 authority or were issued Commission orders requiring firearms background checks.	Paragraph (c) would define the applicability of § 73.18 to licensees or certificate holders who have applied for or received Commission approval of stand-alone preemption authority or combined enhanced-weapons and preemption authority [see considerations below for § 73.19(c) on the applicability of licensee and certificate holder under this proposed rule]. Note: portions of this section would apply to licensee or certificate holder who has applied for, but not yet received preemption authority (e.g., requirements for submission of fingerprints) or those portions that would only apply to licensees or certificate holders who have received NRC approval of their application (e.g., requirements for removal of security personnel who have not yet satisfactorily completed a firearms background check). This section would also apply to power reactor and Category I SSNM licensees or certificate holders issued Commission orders requiring completion of firearms background checks [see consideration for paragraph (b)(2) above].
§ 73.18(d) *Firearms background check requirements*. A firearms background check for security personnel must include – (1) A check of the individual's fingerprints against the Federal Bureau of Investigation's (FBI's) fingerprint system; and (2) A check of the individual's identifying information against the FBI's National Instant Criminal Background Check System (NICS).	Paragraph (d) would identify the two components of a firearms background check that are required by section 161A (i.e., a fingerprint check and a NICS check). The NICS was established pursuant to section 103.(b) of the Brady Handgun Violence Prevention Act (Pub L. 103-159) and is maintained by the FBI.

§ 73.18(e) *Firearms background check submittals*. (1) Licensees and certificate holders shall submit to the NRC, in accordance with § 73.4, for all security personnel requiring a firearms background check under this section - (i) A set of fingerprints, in accordance with paragraph (n) of this section, and (ii) A completed NRC Form 754.	Paragraph (e) would indicate the process for submitting to the NRC the two components of the firearms background check. Accomplishment of the NICS check would be based upon information submitted by the licensee or certificate holder to the NRC under new NRC Form 754 (see Section VIII of this notice for further information on this NRC Form).
§ 73.18(e)(2) Licensees and certificate holders shall retain a copy of all NRC Forms 754 submitted to the NRC for a period of one (1) year subsequent to the termination of an individual's access to covered weapons or to the denial of an individual's access to covered weapons.	Paragraph (e)(2) would establish the records retention requirements for submitted NRC Forms 754.
§73.18(f) *NICS portion of a firearms background check*. The NRC will forward the information contained in the submitted NRC Forms 754 to the FBI for evaluation against the NICS. Upon completion of the NICS check, the FBI will inform the NRC of the results with one of three responses under 28 CFR part 25; "proceed," "denied," or "delayed," and the associated NICS transaction number. The NRC will forward these results and the associated NICS transaction number to the submitting licensee or certificate holder. The licensee or certificate holder shall provide these results to the individual who completed the NRC Form 754.	Paragraph (f) would indicate that the NRC is forwarding the information from submitted NRC Forms 754 to the FBI for evaluation against the NICS. The FBI will return one of the three results from the NICS check (per the FBI's regulations) and a NICS transaction number. The NRC will forward this returned information to the submitting licensee or certificate holder for forwarding to the individual security officer. The NICS transaction number is necessary for any future communications with the FBI on the NICS check (e.g., an individual's appeal of a "denied" NICS response).
§ 73.18(g) *Satisfactory and adverse firearms background checks*. (1) A satisfactorily completed firearms background check means a "proceed" response for the individual from the NICS. (2) An adversely completed firearms background check means a "denied" or "delayed" response from the NICS.	Paragraph (g) would set forth the criteria for a satisfactory firearms background check based upon the specific NICS response. The fingerprint checks mandated by section 161A support the accomplishment of the NICS check and resolution of any adverse NICS records; therefore, the NRC would not specify a [satisfactory or adverse] completion criteria for the fingerprint portion of the firearms background check.

§ 73.18(h) *Removal from access to covered weapons* Licensees or certificate holders who have received NRC approval of their application for § 73.19 authority shall ensure security personnel are removed from duties requiring access to covered weapons upon the licensee's or certificate holder's knowledge of any disqualifying status or the occurrence of any disqualifying events under 18 U.S.C. 922(g) or (n), and the ATF's implementing regulations in 27 CFR part 478.	Paragraph (h) would require the licensee or certificate holder to remove personnel who are prohibited from possessing or receiving firearms from duties requiring access to covered weapons. Disqualifying status or occurrences are found under the United States Code, Title 18, Section 922 and ATF's implementing regulations (see 27 CFR 478.32 and 478.11). See also considerations for § 73.18(b)(5).
§ 73.18(i) [Reserved].	Paragraph (i) would not be used to avoid confusion with the use of sub-sub paragraph (i).
§ 73.18(j) *Security personnel responsibilities*. Security personnel assigned duties requiring access to covered weapons shall promptly [within three (3) working days] notify their employing licensee's or certificate holder's security management (whether directly employed by the licensee or certificate holder or employed by a security contractor to the licensee or certificate holder) of the existence of any disqualifying status or upon the occurrence of any disqualifying events listed under 18 U.S.C. 922(g) or (n), and the ATF's implementing regulations in 27 CFR part 478 that would prohibit them from possessing or receiving a covered weapon.	Paragraph (j) would require security personnel who become prohibited from possessing or receiving firearms due to a disqualifying status or occurrence of a disqualifying event to notify their licensee or certificate holder within three (3) days of this fact. This paragraph would work in conjunction with the requirements of paragraphs (k), (m), and (n) and would require security personnel to self report the occurrence of any disqualifying status or events.

§ 73.18(k) *Awareness of disqualifying events*. Licensees and certificate holders who have received NRC approval of § 73.19 authority shall include within their NRC-approved security training and qualification plans instruction on – (1) Disqualifying status or events specified in 18 U.S.C. 922(g) and (n), and ATF's implementing regulations in 27 CFR part 478 (including any applicable definitions) identifying categories of persons who are prohibited from possessing or receiving any covered weapons; and (2) The continuing responsibility of security personnel assigned duties requiring access to covered weapons to promptly notify their employing licensee or certificate holder of the occurrence of any disqualifying events.	Paragraph (k) would require licensees and certificate holders to train security personnel on disqualifying status or events to facilitate self reporting of such status or events by security personnel under paragraph (j). And to train security personnel on their ongoing responsibility to report disqualifying status or events to their licensee or certificate holder.
§ 73.18(l) [Reserved].	Paragraph (l) would not be used to avoid confusion with the use of sub-paragraph (1) [see also paragraph (i) above].
§ 73.18(m) *Notification of removal*. Within 72 hours after taking action to remove security personnel from duties requiring access to covered weapons, because of the existence of any disqualifying status or the occurrence of any disqualifying event – other than due to the prompt notification by the security officer under paragraph (j) of this section – licensees and certificate holders who have received NRC approval of § 73.19 authority shall notify the NRC Operations Center of such removal actions, in accordance with appendix A of this part.	Paragraph (m) would require licensees or certificate holders to report instances where security personnel (with current access to weapons) are removed from armed duties because of the occurrence of any disqualifying status or event. The timeliness of this notification would be based upon the need for appropriate NRC followup of a potential criminal violation, rather than the followup necessary for an ongoing security event (i.e., the individual no longer has access to covered weapons). Appendix A provides contact information for the NRC Operations Center.
§ 73.18(n) *Reporting violations of law*. The NRC will promptly report suspected violations of Federal law to the appropriate Federal agency or suspected violations of State law to the appropriate State agency.	Paragraph (n) would indicate that if the NRC becomes aware of suspected violations of criminal law (e.g., a prohibited person actually possessing weapons as a security officer) it is obligated to report suspected violations of Federal or State law to the appropriate government agency or agencies.

§ 73.18(o) *Procedures for processing of fingerprint checks*. (1) Licensees and certificate holders who have applied for § 73.19 authority, using an appropriate method listed in § 73.4, shall submit to the NRC's Division of Facilities and Security one (1) completed, legible standard fingerprint card (Form FD-258, ORIMDNRCOOOZ) or, where practicable, other fingerprint record for each individual requiring a firearms background check, to the NRC's Director, Division of Facilities and Security, Mail Stop T6-E46, ATTN: Criminal History Check. Copies of this form may be obtained by writing the Office of Information Services, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, by calling (301) 415-5877, or by e-mail to FORMS@nrc.gov. Guidance on what alternative formats, including electronic submissions, may be practicable are referenced in § 73.4.	Paragraph (o) would prescribe the location, method, and requirements for submission of fingerprints to the NRC as part of a firearms background check. The proposed language would be essentially identical to that contained to the current fingerprint submission requirements under the current access authorization regulations in § 73.57(d).
§ 73.18(o)(2) Licensees and certificate holders shall indicate on the fingerprint card or other fingerprint record that the purpose for this fingerprint check is the accomplishment of a firearms background check.	See considerations for § 73.18(o). This provision will permit proper internal routing of fingerprints within the FBI's Criminal Justice Information Services Division to support the NICS checks.
§ 73.18(o)(3) Licensees and certificate holders shall establish procedures to ensure that the quality of the fingerprints taken results in minimizing the rejection rate of fingerprint cards or records due to illegible or incomplete information.	See considerations for § 73.18(o).

§ 73.18(o)(4) The Commission will review fingerprints for firearms background checks for completeness. Any Form FD-258 or other fingerprint record containing omissions or evident errors will be returned to the licensee or certificate holder for corrections. The fee for processing fingerprint checks includes one (1) free re-submission if the initial submission is returned by the FBI because the fingerprint impressions cannot be classified. The one (1) free re-submission must have the FBI Transaction Control Number reflected on the re-submission. If additional submissions are necessary, they will be treated as an initial submittal and require a second payment of the processing fee. The payment of a new processing fee entitles the submitter to an additional free re-submittal, if necessary. Previously rejected submissions may not be included with the third submission because the submittal will be rejected automatically. Licensees and certificate holders may wish to consider using different methods for recording fingerprints for resubmissions, if difficulty occurs with obtaining a legible set of impressions.	See considerations for § 73.18(o).

§ 73.18(o)(5)(i) Fees for the processing of fingerprint checks are due upon application. Licensees and certificate holders shall submit payment with the application for the processing of fingerprints, and payment must be made by corporate check, certified check, cashier's check, money order, or electronic payment, made payable to "U.S. NRC."[a] Combined payment for multiple applications is acceptable. (ii) The application fee is the sum of the user fee charged by the FBI for each fingerprint card or other fingerprint record submitted by the NRC on behalf of a licensee or certificate holder, and an administrative processing fee assessed by the NRC. The NRC processing fee covers administrative costs associated with NRC handling of licensee and certificate holder fingerprint submissions. The Commission publishes the amount of the fingerprint check application fee on the NRC's public Web site.[b] The Commission will directly notify licensees and certificate holders who are subject to this regulation of any fee changes. Footnotes: [a] For guidance on making electronic payments, contact the NRC's Security Branch, Division of Facilities and Security, Office of Administration at (301) 415-7404. [b] For information on the current fee amount, refer to the Electronic Submittals page at http://www.nrc.gov/site-help/eie.html and select the link for the Criminal History Program.	See considerations for § 73.18(o).
§ 73.18(o)(6) The Commission will forward to the submitting licensee or certificate holder all data received from the FBI as a result of the licensee's or certificate holder's application(s) for fingerprint background checks, including the FBI's fingerprint record.	See considerations for § 73.18(o).

§ 73.18(p) *Appeals and correction of erroneous system information*. (1) Individuals who require a firearms background check under this section and who receive a "denied" NICS response or a "delayed" NICS response may not be assigned duties requiring access to covered weapons during the pendency of an appeal of the results of the check or during the pendency of providing and evaluating any necessary additional information to the FBI to resolve the "delayed" response, respectively. (2) Licensees and certificate holders shall provide information on the FBI's procedures for appealing a "denied" response to the denied individual or on providing additional information to the FBI to resolve a "delayed" response. (3) An individual who receives a "denied" or "delayed" NICS response to a firearms background check under this section may request the reason for the response from the FBI. The licensee or certificate holder shall provide to the individual who has received the "denied" or "delayed" response the unique NICS transaction number associated with the specific firearms background check. (4) These requests for the reason for a "denied" or "delayed" NICS response must be made in writing, and must include the NICS transaction number. The request must be sent to the Federal Bureau of Investigation; NICS Section; Appeals Service Team, Module A-1; PO Box 4278; Clarksburg, WV 26302-9922. The FBI will provide the individual with the reasons for the "denied" response or "delayed" response. The FBI will also indicate whether additional information or documents are required to support an appeal or resolution, for example, where there is a claim that the record in question does not pertain to the individual who was denied.	Paragraph (p)(1) would indicate that individuals who have received a "denied" response or a "delayed" response may not be assigned duties requiring access to covered weapons during their appeal of the denial or resolution of the delay. Paragraph (p)(2) would indicate that the licensee or certificate holder will provide information on the FBI's appeals process to the denied individual. The NRC and FBI are considering creating a brochure describing the appeals process or resolution process that would be similar to the FBI's current brochure [describing the NICS appeals process] provided by federal firearms licensees to individuals receiving a "denied" NICS response (see example at the FBI's NICS information website at http://www.fbi.gov/hq/cjisd/nics/index.htm). Paragraph (p)(3) would indicate that the individual who receives a "denied" or "delayed" response must personally make any requests to the FBI on the reason for the NICS response; and the licensee or certificate holder may not make such requests upon the individual's behalf. Paragraph (p)(4) would provide the FBI's address for correspondence. Additionally, in response to the individual's request the FBI would provide the person the reason for the denial or the delay to facilitate any appeals or to facilitate providing supplemental information to resolve a "delayed" response.

§ 73.18(p)(5) If the individual wishes to challenge the accuracy of the record upon which the "denied" or "delayed" response is based, or if the individual wishes to assert that his or her rights to possess or receive a firearm have been restored by lawful process, he or she may make application first to the FBI. The individual shall file an appeal of a “denied” response or file a request to resolve a "delayed" response within 45 calender days of the date the NRC forwards the results of the firearms background check to the licensee or certificate holder. The appeal or request must include appropriate documentation or record(s) establishing the legal and/or factual basis for the challenge. Any record or document of a court or other government entity or official furnished in support of an appeal must be certified by the court or other government entity or official as a true copy. The individual may supplement their initial appeal or request – subsequent to the 45 day filing deadline – with additional information as it becomes available, for example, where obtaining a true copy of a court transcript may take longer than 45 days. The individual should note in their appeal or request any information or records that are being obtained, but are not yet available. (6) If the individual is notified that the FBI is unable to resolve the appeal, the individual may then apply for correction of the record directly to the agency from which the information forming the basis of the denial was originated. If the individual is notified by the originating agency, that additional information or documents are required the individual may provide them to the originating agency. If the record is corrected as a result of the appeal to the originating agency, the individual may so notify the FBI and submit written proof of the correction.	Paragraph (p)(5) would set a time limit for filing an initial appeal of a "denied" response or to request resolution of a "delayed" response to encourage timely resolution of such cases and facilitate FBI disposition of interim records. The individual filing the appeal would be required to set forth the basis for the appeal and provide information supporting their claim. Copies of records would be required to be true copies (i.e., certified by a court or other government entity). Because some supplemental information may take longer than 45 days to obtain, individuals filling an appeal or requesting resolution should not delay their filing in order to gather all necessary information, but would indicate that additional supporting information will be forthcoming. Paragraph (p)(6) would indicate that if an individual cannot resolve a record with the FBI, the individual may apply to the originating agency to correct the record and notify the FBI of those results. The originating agency may respond to the individual's application by addressing the individual's specific reasons for the challenge, and by indicating whether additional information or documents are required. If the record is corrected as a result of the appeal to the originating agency, the individual may so notify the FBI, which would, in turn, verify the record correction with the originating agency (assuming the originating agency has not already notified the FBI of the correction) and take all necessary steps to correct the record in the NICS system.

§ 73.18(p)(7) An individual who has satisfactorily appealed a "denied" response or resolved a "delayed" response may provide written consent to the FBI to maintain information about himself or herself in a Voluntary Appeal File (VAF) to be established by the FBI and checked by the NICS for the purpose of preventing the erroneous denial or extended delay by the NICS of any future NICS checks. (8) Individuals appealing a "denied" response or resolving a “delayed” response are responsible for providing the FBI any additional information the FBI requires to resolve the “delayed” response.	Paragraph (p)(7) would indicate that an individual who has successfully resolved a "denied" or "delayed" response may consent to the FBI maintaining information about himself or herself in the FBI's VAF (i.e., the basis for the successful resolution). The FBI will issue such individuals a VAF number that can be entered on an NRC Form 754 or ATF Form 4417 to prevent repetition of excessive delays in completing any future NICS checks (both for checks as security personnel and for checks of individuals engaging in a firearms transaction as a private person). A VAF file would be used only by the NICS for this purpose. The FBI would remove all information in the VAF pertaining to an individual upon receipt of a written request by that individual. However, the FBI may retain such information contained in the VAF as long as needed to pursue cases of identified misuse of the system. If the FBI finds a disqualifying record on the individual after his or her entry into the VAF, the FBI may remove the individual's information from the file. Paragraph (p)(8) would indicate that the responsibility for providing any necessary additional information to the FBI to appeal the "denied" response or resolve the "delayed" rests with the individual, not with the FBI.
§ 73.19 **Authorization for preemption of firearms laws and use of enhanced weapons.** (a) *Purpose*. This section sets forth the requirements for licensees and certificate holders to obtain NRC approval to use the expanded authorities provided under section 161A of the Atomic Energy Act of 1954, as amended (AEA), in protecting NRC-designated facilities, radioactive material, or other property. These authorities include “preemption authority” and “enhanced-weapons authority.”	This new section would implement the provisions of new section 161A of the AEA with respect to preemption authority alone or combined enhanced-weapons authority and preemption authority. This section would permit, but not require, selected classes of licensees and certificate holders to apply to the NRC for these authorities. Paragraph (a) would provide the overall purpose and indicate that this section applies to defending NRC-designated facilities, radioactive material, or other property.

§ 73.19(b) *General Requirements*. Licensees and certificate holders listed in paragraph (c) of this section may apply to the NRC, in accordance with the provisions of this section, to receive stand-alone preemption authority or combined enhanced weapons authority and preemption authority. (1) Preemption authority, as provided in section 161A of the AEA, means the authority of the Commission to permit licensees or certificate holders, or the designated security personnel of the licensee or certificate holder, to transfer, receive, possess, transport, import, or use one (1) or more category of standard and enhanced weapons, as defined in § 73.2, notwithstanding any local, State, or certain Federal firearms laws (including regulations). (2) Enhanced weapons authority, as provided in section 161A of the AEA, means the authority of the Commission to permit licensees or certificate holders, or the designated security personnel of the licensee or certificate holder, to transfer, receive, possess, transport, import, and use one (1) or more category of enhanced weapons, as defined in § 73.2, notwithstanding any local, State, or certain Federal firearms laws (including regulations).	Paragraph (b) would contain general requirements and overview of the advantages of these two authorities. The ability of licensees and certificate holders to apply to the NRC for stand-alone preemption authority or combined enhanced-weapons authority and preemption authority would be limited to the classes of licensees set forth in paragraph (c) of this section. Licensees and certificate holders may apply for preemption authority alone. However, licensees and certificate holders who apply for enhanced-weapons authority would also be required to apply for preemption authority, because of restrictions on the possession of enhanced weapons require the preemption of certain regulations. The NRC would create this separate, but parallel, structure to provide licensees with flexibility in choosing security capabilities versus security costs. Paragraphs (b)(1) and (b)(2) provide definitions of these two authorities.

§ 73.19(b)(3) Prior to receiving NRC approval of enhanced-weapons authority, the licensee or certificate holder must have applied for and received NRC approval for preemption authority, in accordance with this section or under Commission orders. (4) Prior to granting either authority the NRC must determine that the proposed use of this authority is necessary in the discharge of official duties by security personnel engaged in protecting – (i) Facilities owned or operated by a licensee or certificate holder and designated by the Commission under paragraph (c) of this section, or (ii) Radioactive material or other property that is owned or possessed by a licensee or certificate holder, or that is being transported to or from an NRC-regulated facility. Before granting such approval, the Commission must determined that the radioactive material or other property is of significance to the common defense and security or public health and safety and has designated such radioactive material or other property under paragraph (c) of this section.	Paragraph (b)(3) would indicate that to receive enhanced-weapons authority, a licensee or certificate holder must also have received preemption authority. Paragraph (b)(4) would describe the criteria of section 161A the Commission must determine are present for a licensee or certificate holder to apply to the NRC for stand-alone preemption authority or combined enhanced-weapons authority and preemption authority for other types of facilities, radioactive material, or other property.

§ 73.19(c) *Applicability*. (1) The following classes of licensees or certificate holders may apply for stand-alone preemption authority – (i) Power reactor facilities; and (ii) Facilities authorized to possess a formula quantity or greater of strategic special nuclear material with security plans subject to §§ 73.20, 73.45, and 73.46. (2) The following classes of licensees or certificate holders may apply for combined enhanced-weapons authority and preemption authority – (i) Power reactor facilities; and (ii) Facilities authorized to possess a formula quantity or greater of strategic special nuclear material with security plans subject to §§ 73.20, 73.45, and 73.46.	Paragraph (c)(1) would limit the types of licensees who could apply for stand-alone preemption authority alone to two classes of NRC-regulated facilities - power reactor facilities and fuel cycle facilities authorized to possess Category I quantities of SSNM. Such SSNM fuel cycle facilities would include: production facilities, spent fuel reprocessing facilities, fuel fabrication facilities, and uranium enrichment facilities. However, they would not include hot cell facilities, independent spent fuel storage installations, monitored retrievable storage installations, geologic repository operations areas, non-power reactors, byproduct material facilities, and the transportation of spent fuel, high level waste, and special nuclear material. Paragraph (c)(2) would also limit the types of licensees who could apply for combined enhanced-weapons authority and preemption authority to these same two classes of licensed facilities. The Commission is proposing under this rulemaking to limit the range of facilities, radioactive material, or other property [for which these authorities are appropriate] to power reactor facilities and fuel cycle facilities authorized to possess Category I quantities of strategic special nuclear material. The Commission would take this approach to be consistent with the scope of this rulemaking. The Commission may consider other types of facilities, radioactive material, or other property as appropriate for these authorities in future rulemakings. Additionally, the Commission would use the parallel structure in paragraph (c) to facilitate future rulemakings. Specifically, the Commission recognizes that enhanced-weapons authority may not be appropriate for all present and future classes of licensees with armed security programs; whereas the applicability of preemption authority to all present and future classes of licensees with armed security programs may be much broader.

§ 73.19(c)(3) With respect to the possession and use of firearms by all other NRC licensees or certificate holders, the Commission's requirements in effect before **[effective date of final rule]** remain applicable, except to the extent those requirements are modified by Commission order or regulations applicable to such licensees and certificate holders.	Paragraph (b)(3) would indicate that the provisions of this section do not supersede existing Commission regulations or orders for non-power reactor and non-Category I SSNM licensees, unless specifically indicated.
§ 73.19(d) *Authorization for stand-alone preemption of firearms laws*. (1) Licensees and certificate holders listed in paragraph (c) of this section may apply to the NRC for the preemption authority described in paragraph (b)(1) of this section. Licensees and certificate holders seeking such authority shall submit an application to the NRC in writing, in accordance with § 73.4, and indicate that the licensee or certificate holder is requesting preemption authority under section 161A of the AEA. (2) Licensees and certificate holders who have applied for preemption authority under this section may begin firearms background checks under § 73.18 for their armed security personnel. (3) Licensees and certificate holders who have applied for preemption authority under this section and who have satisfactorily completed firearms background checks for a sufficient number of security personnel (to implement their security plan while meeting security personnel fatigue requirements of this chapter or Commission order) shall notify the NRC, in accordance with § 73.4, of their readiness to receive NRC approval of preemption authority and implement all the provisions of § 73.18.	Paragraph (d)(1) would describe the process for a licensee or certificate holder to apply for preemption authority. This would be a voluntary action. Based upon the Commission's conclusion that the classes of facilities listed under paragraph (c) are appropriate for the use of such preemption authority, no additional documentation or supporting information would be required by a licensee or certificate holder to apply for preemption authority other than the licensee or certificate holder is included within the list of licenses and certificate holders in paragraph (c). Paragraph (d)(2) would permit licensees and certificate holders who have applied for preemption authority to begin submitting their security personnel for firearms background checks under § 73.18. Paragraph (c)(3) would require licensees and certificate holders who applied for preemption authority to subsequently notify the NRC of their readiness to fully implement § 73.18 without adverse impact on the security organization (i.e., the provisions in § 73.18 requiring removal from armed duties of personnel with a"denied" or "delayed" response would not adversely affect the licensee's or certificate holder's security organization).

§ 73.19(d)(4) Based upon the licensee's or certificate holder's readiness notification and any discussions with the licensee or certificate holder, the NRC will document in writing to the licensee or certificate holder that the Commission has approved or disapproved the licensee's or certificate holder's application for preemption authority.	Paragraph (d)(4) would indicate that the NRC will rely upon the licensee's or certificate holder's determination that sufficient numbers of its security personnel have satisfactorily passed the firearms background check to fully implement the provisions of § 73.18. The NRC would document in writing its approval or disapproval of the licensee's or certificate holder's application for preemption authority. The NRC may also rely upon discussions with the licensee or certificate holder to reach a conclusion.
§ 73.19(e) *Authorization for use of enhanced weapons*. (1) Licensees and certificate holders listed in paragraph (c)(2) of this section may apply to the NRC for enhanced-weapons authority described in paragraph (a)(2) of this section. Licensees and certificate holders applying for enhanced-weapons authority shall have also applied for preemption authority. Licensees and certificate holders may make these applications concurrently. (2) Licensees and certificate holders seeking enhanced-weapons authority shall submit an application to the NRC, in accordance with § 73.4, indicating that the licensee or certificate holder is requesting enhanced-weapons authority under section 161A of the AEA. Licensees and certificate holders shall also include with their application - (i) The additional information required by paragraph (f) of this section; (ii) The date they applied to the NRC for preemption authority (if not concurrent with the application for enhanced weapons authority); and (iii) If applicable, the date when the licensee or certificate holder received NRC approval of their application for preemption authority under this section or via Commission order.	Paragraph (e)(1) would describe the process for a licensee or certificate holder to apply for combined enhanced-weapons authority and preemption authority. A licensee or certificate holder would be permitted to apply for preemption authority in conjunction with an application for enhanced-weapons authority, or the licensee or certificate holder may apply for preemption authority first. Only the classes of licensees and certificate holders listed under paragraph (c)(2) would be permitted to apply for combined enhanced-weapons authority and preemption authority. Paragraph (e)(2) would require a licensee or certificate holder to include specific information with their application as set forth in § 73.19(f). The licensee or certificate holder would also be required to include information on the date they applied for, and/or received NRC approval of their application for preemption authority under § 73.19, or under Commission order prior to the effective date of a final rule.

§ 73.19(e)(3) The NRC will document in writing to the licensee or certificate holder that the Commission has approved or disapproved the licensee's or certificate holder's application for enhanced-weapons authority. The NRC must approve, or have previously approved, a licensee's or certificate holder's application for preemption authority under paragraph (d) of this section, or via Commission order, to approve the application for enhanced weapons authority.	Paragraph (e)(3) would indicate that the NRC would document in writing the approval or disapproval of an application for combined enhanced-weapons authority and preemption authority. The NRC's approval would also indicate the total numbers, types, and calibers of enhanced weapons that are approved for a specific licensee or certificate holder.

§ 73.19(e)(4) Licensees and certificate holders who have applied to the NRC for and received enhanced-weapons authority shall then apply to the U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) for a federal firearms license (FFL) and also register under the National Firearms Act (NFA) in accordance with ATF regulations under 27 CFR parts 478 and 479 to obtain the enhanced weapons. Licensees and certificate holders shall include a copy of the NRC's written approval with their NFA registration application.	Paragraph (e)(4) would indicate that after the licensee or certificate holder has received NRC approval of its application to use enhanced weapons, it must then apply to ATF to obtain a FFL and also register under the NFA to obtain these weapons. Because ATF has indicated it would rely upon the NRC's technical evaluation [on whether the specific weapons listed in the NRC's approval are appropriate for the licensee or certificate holder] in processing the licensee's or certificate holder's NFA registration application, licensees and certificate holders would include a copy of the NRC's approval with their NFA registration application. This paragraph would require licensees to obtain a FFL in addition to registering under the NFA. Based upon conversations with ATF, the NRC understands that while ATF's regulations do not mandate that persons who obtain NFA weapons also have an FFL, NRC licensees and certificate holders desiring to obtain enhanced weapons would benefit from status an ATF FFL. Advantages would include reduced time to process requests to transfer NFA weapons to or from the licensee or certificate holder (e.g., initial receipt, repair, or disposition), simplification of the ATF's review of an NFA registration application, and elimination of transfer taxes for NFA-weapons transactions. The NRC also understands that status as an FFL would create obligations for such licensee's and certificate holders. Obligations would include payment of an annual special occupational tax, additional recordkeeping requirements, and a requirement to permit ATF inspectors access to the licensee's or certificate holder's facilities possessing enhanced weapons to inspect ATF-licensed weapons and corresponding records.

§ 73.19(f) *Application for enhanced-weapons authority additional information*. (1) Licensees and certificate holders applying to the Commission for enhanced-weapons authority under paragraph (e) of this section shall also submit to the NRC for prior review and written approval new, or revised, physical security plans, security personnel training and qualification plans, safeguards contingency plans, and safety assessments incorporating the use of the specific enhanced weapons the licensee or certificate holder intends to use. These plans and assessments must be specific to the facility, radioactive material, or other property being protected.	Paragraph (f)(1) would describe the additional information a licensee or certificate holder would be required to submit along with their application for preemption and enhanced-weapons authority. This information would be submitted to the NRC for prior review and approval and would describe and address the specific weapons to be employed. In addition to addressing the enhanced weapons in the security, training and qualification, and safeguards contingency plans, a licensee or certificate holder would also provide a safety assessment on the use of the specific enhanced weapons to be employed. Licensees and certificate holders who apply for authority alone under paragraph (d) would not be subject to the requirements of paragraph (f).
§ 73.19(f)(2) In addition to other requirements set forth in this part, these plans and assessments must – (i) For the physical security plan, identify the specific types or models, calibers, and numbers of enhanced weapons to be used; (ii) For the training and qualification plan, address the training and qualification requirements to use these specific enhanced weapons; and (iii) For the safeguards contingency plan, address how these enhanced and any standard weapons will be employed by the licensee's or certificate holder's security personnel in meeting the NRC-required protective strategy, including tactical approaches and maneuvers.	Paragraph (e)(2) would describe specific information the license or certificate holder would include in the plans and assessments accompanying the application for enhanced-weapons authority. The paragraph would also describe the scope of the safety assessments and would require evaluation of both onsite and offsite impacts from the use of the specific enhanced weapons to be employed. The safety assessment would be required to only address the enhanced weapons the license or certificate holder intends to employ.

§ 73.19(f)(2)(iv) For the safety assessment – (A) Assess any potential safety impact on the facility, radioactive material, or other property from the use of these enhanced weapons; (B) Assess any potential safety impact on public or private facilities, public or private property, or on members of the public in areas outside of the site boundary from the use of these enhanced weapons; and (C) Assess any potential safety impact on public or private facilities, public or private property, or on members of the public from the use of these enhanced weapons at training facilities intended for proficiency demonstration and qualification purposes.	See considerations for § 73.19(f)(2).
§ 73.19(f)(3) The licensee's or certificate holder's training and qualification plan on possessing, storing, maintaining, qualifying on, and using enhanced weapons must include information from applicable firearms standards developed by nationally-recognized firearms organizations or standard setting bodies or standards developed by Federal agencies, such as: the U.S. Department of Homeland Security's Federal Law Enforcement Training Center, the U.S. Department of Energy's National Training Center, and the U.S. Department of Defense. (4) Licensees or certificate holders shall submit any new or revised plans and assessments for prior NRC review and written approval notwithstanding the provisions of §§ 50.54(p), 70.32(e), and 76.60 of this chapter which otherwise permit a license or certificate holder to make changes to such plans "that would not decrease their effectiveness" without prior NRC review.	Paragraph (f)(3) would specify acceptable standards for the licensee or certificate holder to use in creating a training and qualification plan for enhanced weapons. This paragraph would not create any new requirements for training standards for standard weapons. Paragraph (f)(4) would require the submission of revised plans for prior NRC review and approval, irrespective of whether the licensee or certificate holder concludes that the use of these enhanced weapons would not cause "a decrease in security effectiveness" under the applicable NRC regulation.

§ 73.19(g) *Completion of training and qualification prior to use of enhanced weapons*. Licensees and certificate holders who have applied for and received enhanced-weapons authority under paragraph (e) of this section shall ensure security personnel complete required firearms training and qualification in accordance with the licensee's or certificate holder's NRC-approved training and qualification plan. Such training must be completed prior to security personnel's use of enhanced weapons to protect NRC-designated facilities, radioactive material, or other property and must be documented in accordance with the requirements of the licensee's or certificate holder's training and qualification plan.	Paragraph (g) would require licensees and certificate holders to ensure security personnel are trained and qualified on the use and employment enhanced weapons before the licensee or certificate holder deploys these enhanced weapons to defend the facility, radioactive material, or other property. Documentation of completion of this training would be consistent with the licensee's or certificate holder's approved training and qualification plan.
§ 73.19(h) *Use of enhanced weapons*. Requirements regarding the use of enhanced weapons by security personnel in the performance of their official duties are contained in §§ 73.46 and 73.55 and in appendices B and C of this part, as applicable.	Paragraph (h) would indicate that § 73.19 does not supercede requirements on the use of weapons under the power reactor and Category I fuel cycle facility security regulations found in Part 73.
§ 73.19(i) [Reserved].	Paragraph (i) would not be used to avoid confusion with the use of sub-sub paragraph (i).
§ 73.19(j) *Notification of adverse ATF findings or notices*. NRC licensees and certificate holders with an ATF federal firearms license (FFL) and/or enhanced weapons shall notify the NRC, in accordance with § 73.4, of instances involving any adverse ATF findings or ATF notices related to their FFL or such weapons.	Paragraph (j) would require NRC licensees or certificate holders to notify NRC, should the licensee or certificate holder receive any adverse findings based upon an ATF inspection, audit, or review of the enhanced weapons possessed by the licensee or certificate holder under an ATF FFL. This would allow the NRC to appropriately respond to any public or media inquiries associated with such findings in a timely manner.

§ 73.2 **Definitions**.	Three new definitions would be added to this section as conforming changes supporting the new §§ 73.18 and 73.19 that would include: *covered weapon*, *enhanced weapon*, and *standard weapon*. The NRC would use these three terms to envelope the weapons, ammunition, and devices listed under section 161A of the AEA. Other new definitions that would be added as conforming changes to this section in support of other regulations (e.g., *safety/security interface* and *target set*) are discussed in other tables in this proposed rule.
Covered weapon means any handgun, rifle, shotgun, short-barreled shotgun, short-barreled rifle, semi-automatic assault weapon, machinegun, ammunition for any such gun or weapon, or large capacity ammunition feeding device as specified under section 161A of the Atomic Energy Act of 1954, as amended. As used here, the terms "handgun, rifle, shotgun, short-barreled shotgun, short-barreled rifle, semi-automatic assault weapon, machinegun, ammunition, or large capacity ammunition feeding device" have the same meaning as set forth for those terms under 18 U.S.C. 921(a). Covered weapons include both enhanced weapons and standard weapons. However, enhanced weapons do not include standard weapons.	A definition for *covered weapon* would be used as an overall term to encompass the firearms (weapons), ammunition, and devices listed in section 161A. The meanings of the specific terms for the firearms, ammunition, or devices encompassed within this definition would have the same meaning for those terms as is those found under Title 18 of the United States Code, Section 921(a) [18 U.S.C. 921(a)].

Enhanced weapon means any short-barreled shotgun, short-barreled rifle, or machinegun. Enhanced weapons do not include destructive devices, including explosives or weapons greater than 50 caliber (i.e., weapons with a bore greater than 1.27 cm [0.5 in] diameter). *Standard weapon* means any handgun, rifle, shotgun, semi-automatic assault weapon, or a large capacity ammunition feeding device.	Definitions for *enhanced weapon* and *standard weapon* would be added to support the differing scope of these new sections. The relationship between covered weapon, enhanced weapon, and standard weapon would be explained. Also, the definition for enhanced weapons would not include destructive devices as defined under ATF's regulations, since the NRC's authority under section 161A of the AEA does not permit licensees or certificate holders to possess destructive devices.

Table 2 - Part 73 Section 73.55
Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.	Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.	This title would be retained.
	(a) Introduction.	This header would be added for formatting purposes.
§ 73.55 By December 2, 1986, each licensee, as appropriate, shall submit proposed amendments to its security plan which define how the amended requirements of Paragraphs (a), (d)(7), (d)(9), and (e)(1) will be met.	(a)(1) By **[date - 180 days - after the effective date of the final rule published in the *Federal Register*]**, each nuclear power reactor licensee, licensed under 10 CFR part 50, shall incorporate the revised requirements of this section through amendments to its Commission-approved Physical Security Plan, Training and Qualification Plan, and Safeguards Contingency Plan, referred to collectively as "approved security plans," and shall submit the amended security plans to the Commission for review and approval.	This requirement would be added to discuss the types of Commission licensees to whom the proposed requirements of this section would apply and the schedule for submitting the amended security plans. The Commission intends to delete the current language, because it applies only to a past rule change that is completed. The proposed requirements of this section would be applicable to decommissioned/ing reactors unless otherwise exempted.
§ 73.55 Each submittal must include a proposed implementation schedule for Commission approval.	(a)(2) The amended security plans must be submitted as specified in § 50.4 of this chapter and must describe how the revised requirements of this section will be implemented by the licensee, to include a proposed implementation schedule.	This requirement would be added to provide a reference to the current § 50.4(b)(4) which describes procedural details relative to the proposed security plan submission requirement.

§ 73.55 The amended safeguards requirements of these paragraphs must be implemented by the licensee within 180 days after Commission approval of the proposed security plan in accordance with the approved schedule.	(a)(3) The licensee shall implement the existing approved security plans and associated Commission orders until Commission approval of the amended security plans, unless otherwise authorized by the Commission.	This requirement would be added to clarify that the licensee must continue to implement the current Commission-approved security plans until the Commission approves the amended plans. The phrase “unless otherwise authorized by the Commission” would provide flexibility to account for unanticipated situations that may affect the licensee's ability to comply with this proposed requirement.
§ 73.55(b)(1)(i) The licensee is responsible to the Commission for maintaining safeguards in accordance with Commission regulations and the licensee's security plan.	(a)(4) The licensee is responsible for maintaining the onsite physical protection program in accordance with Commission regulations and related Commission-directed orders through the implementation of the approved security plans and site implementing procedures.	This requirement would retain the current requirement that the licensee is responsible for meeting Commission regulations and the approved security plans. The phrase “through the implementation of the approved security plans and site implementing procedures” would be added to describe the relationship between Commission regulations, the approved security plans, and implementing procedures. The word "safeguards" would be replaced with the phrase "physical protection program" to more accurately focus this requirement to the security program rather than the broad "safeguards" which includes safety.

		The Commission views the approved security plans as the mechanism through which the licensee meets Commission requirements through implementation, therefore, the licensee is responsible to the Commission for this performance.
	(a)(5) Applicants for an operating license under the provisions of part 50 of this chapter, or holders of a combined license under the provisions of part 52 of this chapter, shall satisfy the requirements of this section before the receipt of special nuclear material in the form of fuel assemblies.	This requirement would be added to describe the proposed requirements for applicants and to specify that these proposed requirements must be met before an applicant's receipt of special nuclear material in the form of fuel assemblies.
	(a)(6) For licenses issued after [effective date of this rule], licensees shall design, construct, and equip the central alarm station and secondary alarm station to equivalent standards.	This requirement would be added to describe the Commission expectations for new reactors. Based on changes to the threat environment the Commission has determined that the functions required to be performed by the central alarm station are a critical element of the licensee capability to satisfy the performance objective and requirements of the proposed paragraph (b) of this section.

		Therefore, to ensure that these critical capabilities are maintained, the Commission has determined that this proposed requirement would be a prudent and necessary measure to ensure the licensee's ability to summon assistance or otherwise respond to an alarm as is currently required by § 73.55(e)(1) and therefore satisfy the performance objective and requirements of the proposed paragraph (b) of this section.
	(a)(6)(i) Licensees shall apply the requirements for the central alarm station listed in paragraphs (e)(6)(v), (e)(7)(iii), and (i)(8)(ii) of this section to the secondary alarm station as well as the central alarm station.	This requirement would be added for consistency with and clarification of the proposed requirement of paragraph (a)(6) of this section. The Commission has determined that these construction standards that were previously applied to only the central alarm station should also be built into the secondary alarm station for new reactor licensees.

	(a)(6)(ii) Licensees shall comply with the requirements of paragraph (i)(4) of this section such that both alarm stations are provided with equivalent capabilities for detection, assessment, monitoring, observation, surveillance, and communications.	This requirement would be added for consistency with and clarification of the proposed requirement of paragraph (i)(4) of this section and to clarify that for new reactors, both the central and secondary alarm stations must be provided "equivalent capabilities" and not simply equivalent "functional" capabilities as is stated in the proposed paragraph (i)(4) of this section. The Commission has determined that these capabilities must be equivalent for new reactors to ensure that the secondary alarm station is redundant to the central alarm station.
§ 73.55(a) General performance objective and requirements.	(b) General performance objective and requirements.	This header would be retained. The proposed requirements of this section are intended to represent the general outline for a physical protection program that would provide an acceptable level of protection if effectively implemented. The proposed actions, standards, criteria, and requirements of this section are intended to be bounded by the description of the design basis threat identified by the Commission in § 73.1.

§ 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.	(b)(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.	This requirement would retain the current performance objective of § 73.55(a) with two minor changes. First, the phrase "an onsite physical protection system" would be replaced with the phrase "a physical protection program" to more clearly state the Commission's view that the physical protection system elements described in this proposed rule combine to make the licensee physical protection program. Second, the word “and” would be replaced with the phrase “to include a” to clarify the Commission's view that the security organization is not considered to be independent of the licensee physical protection program but rather, is a component of that program.

§ 73.55(a) The physical protection system shall be designed to protect against the design basis threat of radiological sabotage as stated in § 73.1(a). § 73.55(h)(4)(iii)(A) Requiring responding guards or other armed response personnel to interpose themselves...	(b)(2) The physical protection program must be designed to detect, assess, intercept, challenge, delay, and neutralize threats up to and including the design basis threat of radiological sabotage as stated in § 73.1(a), at all times.	This requirement would contain a substantial revision to provide a more detailed and performance based requirement for the design of the licensee physical protection program. Most significantly, the word "interpose" would be replaced with the words “detect, assess, intercept, challenge, delay, and neutralize". The current requirement of § 73.55(h)(4)(iii)(A) requires the licensee to "interpose" for the purpose of preventing radiological sabotage, however, the definition of “radiological sabotage” stated in § 73.2 does not contain a performance based element by which the Commission can measure this capability and therefore, this proposed requirement would provide the six performance based elements or capabilities "detect, assess, intercept, challenge, delay, and neutralize." The first element, “detect”, would be provided through the use of detection equipment, patrols, access controls, and other program elements required by this proposed rule and would provide notification to the licensee that a potential threat is present and where the threat is located.

		The second element, “assess”, would provide a mechanism through which the licensee would identify the nature of the threat detected. This would be accomplished through the use of video equipment, patrols, and other program elements that would be required by this proposed rule and would provide the licensee with information about the threat upon which the licensee would determine how to respond. The third, fourth, and fifth elements would comprise the component actions of response and would be provided by personnel trained and equipped in accordance with a response strategy. The third element “intercept” would be the act of placing a person at an intersecting defensive position directly in the path of advancement taken by the threat, and between the threat and the protected target or target set element. The fourth element “challenge” would be to verbally or physically confront the threat to impede, halt, or otherwise interact with the threat with the intent of preventing further advancement of the threat towards the protected target or target set element.

		The fifth element "delay" would be to take necessary actions to counter any attempt by the threat to advance towards the protected target or target set element. The sixth element “neutralize” would be to place the threat in a condition from which the threat no longer has the potential to, or capability of, doing harm to the protected item. The Commission does not intend to suggest that the action, "neutralize", would require the application of “deadly force” in all instances. The phrase "threat of radiological sabotage" would be replaced with the phrase “threats up to and including the design basis threat of radiological sabotage" to clarify the Commission's view that the licensee must provide protection against any element of the design basis threat, to include those that do not rise to the full capability of the design basis threat.

§ 73.55(a) To achieve this general performance objective, the onsite physical protection system and security organization must include, but not necessarily be limited to, the capabilities to meet the specific requirements contained in paragraphs (b) through (h) of this section. § 73.55(e)(1) ...so that a single act cannot remove the capability of calling for assistance or otherwise responding to an alarm.	(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.	This requirement would retain and revise two current requirements to provide a performance based requirement for the design of the physical protection program. The first significant revision would expand the current requirement for alarm stations to be protected against a single act, and would require that the licensee physical protection program be designed to ensure that a single act can not disable the personnel, equipment, or systems necessary to prevent significant core damage and spent fuel sabotage which would result in the loss of the capability to prevent radiological sabotage. The Commission's view is that because of changes to the threat environment, it is necessary to emphasize the "remove the capability" requirement of the current § 73.55(e)(1) such that the single act protection requirement would apply to personnel, equipment, and systems required to perform specific functions that if disabled would remove the licensee capability to prevent radiological sabotage. The second significant revision would provide a measurable and performance based requirement against which the Commission would measure the effectiveness of the licensee's physical protection program to prevent radiological sabotage.

		The Commission's view is that the goal of the licensee's physical protection program must include an acceptable safety margin to assure that the performance objective of public health and safety is met. This safety margin would be established by designing and implementing a physical protection program that protects against radiological sabotage by preventing significant core damage and spent fuel sabotage which describes the undesirable consequences that could result from the destruction of a target set or all elements of a target set and would be a precursor to radiological sabotage. The Commission's view is that significant damage to the core or sabotage to spent fuel would result in a condition in which the performance objective of "High Assurance" could no longer be provided and therefore, prevention of significant core damage and spent fuel sabotage are a measurable performance criteria against which the Commission would evaluate the effectiveness of the licensee physical protection program.

		The phrase "as bounded by the design basis threat" would be used to clarify the Commission's view that the licensee must ensure that the physical protection program is designed to protect against the design basis threat and all other threats that do not rise to the level of the design basis threat. The phrase "the capabilities to meet the specific requirements contained in paragraphs (b) through (h) of this section" would be replaced by the phase “implemented to satisfy the requirements of this section” to account for the reformatting of this proposed rule and to describe the Commission view that the licensee is responsible to implement Commission requirements through the approved security plans and procedures.
	(b)(4) The physical protection program must include diverse and redundant equipment, systems, technology, programs, supporting processes, and implementing procedures.	This requirement would be added to apply defense-in-depth concepts as part of the physical protection program to ensure the capability to meet the performance objective of the proposed paragraph (b)(1) of this section is maintained in the changing threat environment. The terms “diverse and redundant” are intended to describe defense-in-depth in a performance based manner and would be a critical element for meeting the proposed requirement for protection against a single act described in the proposed paragraph (b)(3) of this section.

§ 73.55(b)(4)(i) Upon the request of an authorized representative of the Commission, the licensee shall demonstrate the ability of the physical security personnel to carry out their assigned duties and responsibilities.	(b)(5) Upon the request of an authorized representative of the Commission, the licensee shall demonstrate the ability to meet Commission requirements through the implementation of the physical protection program, including the ability of armed and unarmed personnel to perform assigned duties and responsibilities required by the approved security plans and licensee procedures.	This requirement would retain the current requirement for demonstration and would contain minor revisions to apply this requirement to the licensee's ability to implement the physical protection program and not be limited to only the ability of security personnel to carry out their duties. This proposed requirement would clarify the Commission's view that the licensee must also demonstrate the effectiveness of plans, procedures, and equipment to accomplish their intended function within the physical protection program.
	(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.	This requirement would be added to specify that this performance evaluation program would be the mechanism by which the licensee would demonstrate the capabilities described by the performance based requirements of the proposed paragraphs (b)(2) through (4) of this section. The phrase "target sets" would be used consistent with the proposed (b)(3) of this section to describe the combination of equipment and operator actions which, if all are prevented from performing their intended safety function or prevented from being accomplished, would likely result in significant core damage (e.g., non-incipient, non-localized fuel melting, and/or core disruption) barring extraordinary action by plant operators.

		A target set with respect to spent fuel sabotage is draining the spent fuel pool leaving the spent fuel uncovered for a period of time, allowing spent fuel heat up and the associated potential for release of fission products.
§ 73.55(d)(7) The licensee shall: (i) Establish an access authorization system...	(b)(7) The licensee shall establish, maintain, and follow an access authorization program in accordance with § 73.56.	This requirement would be retained and revised to require the licensee to provide an Access Authorization Program.
	(b)(7)(i) In addition to the access authorization program required above, and the fitness-for-duty program required in part 26 of this chapter, each licensee shall develop, implement, and maintain an insider mitigation program.	This proposed requirement would be added to establish the insider mitigation program (IMP). The licensee's IMP should integrate specific elements of the licensee AA and FFD programs to focus those elements on identifying potential insider threats and denying the opportunity for an insider to gain or retain access at an NRC licensed facility.

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

		The Commission has determined that no one element of the physical protection program, access authorization program, or fitness-for-duty program would, by itself, provide the level of protection against the insider necessary to meet the performance objective of the proposed paragraph (b) and therefore, the effective integration of these three programs is a necessary requirement to achieve defense-in-depth against the potential insider.
	(b)(8) The licensee shall ensure that its corrective action program assures that failures, malfunctions, deficiencies, deviations, defective equipment and nonconformances in security program components, functions, or personnel are promptly identified and corrected. Measures shall ensure that the cause of any of these conditions is determined and that corrective action is taken to preclude repetition.	This requirement would be added to provide a performance based requirement to ensure that the licensee implements and completes the required corrective actions in a timely manner and that actions would be taken to correct the cause of the problem to ensure that the problem would not be repeated.

	(c) Security plans.	This header would be added for formatting purposes.
	(c)(1) Licensee security plans. Licensee security plans must implement Commission requirements and must describe:	This requirement would be added to describe the purpose of the licensee Physical Security Plan, Training & Qualification Plan, and Safeguards Contingency Plan in a performance based requirement and to introduce the general types of information to be discussed.
	(c)(1)(i) How the physical protection program will prevent significant core damage and spent fuel sabotage through the establishment and maintenance of a security organization, the use of security equipment and technology, the training and qualification of security personnel, and the implementation of predetermined response plans and strategies; and	This requirement would be added to describe the performance based requirement to be met by the physical protection program and the basic elements of the system that must be described in the security plans.
	(c)(1)(ii) Site-specific conditions that affect implementation of Commission requirements.	This requirement would be added to reflect the Commission's view that licensees must focus attention on site-specific conditions in the development and implementation of site plans, procedures, processes, response strategies, and ultimately, the licensee capability to achieve the performance objective of the proposed paragraph (b)(1) of this section.

	(c)(2) Protection of security plans. The licensee shall protect the approved security plans and other related safeguards information against unauthorized disclosure in accordance with the requirements of § 73.21.	This requirement would be added to emphasize the requirements for the protection of safeguards information in accordance with the requirements of § 73.21.
	(c)(3) Physical security plan.	This header would be added for formatting purposes.
	(c)(3)(i) The licensee shall establish, maintain, and implement a Commission-approved physical security plan that describes how the performance objective and requirements set forth in this section will be implemented.	This requirement would be added to specify the requirement for a physical security plan.
	(c)(3)(ii) The physical security plan must describe the facility location and layout, the security organization and structure, duties and responsibilities of personnel, defense-in-depth implementation that describes components, equipment and technology used.	This requirement would be added to describe the general content of the physical security plan and specify the general types of information to be addressed. Because the specifics of defense-in-depth required by the proposed § 73.55(b)(4) would vary from site-to-site, the terms “components,” “equipment” and “technology” would be used to provide flexibility.
	(c)(4) Training and qualification plan.	This header would be added for formatting purposes.

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

		The phrase ”meet the requirements of this paragraph“ would be replaced by the phrase “possess the knowledge, skills, and abilities required to effectively carry out their assigned duties and responsibilities” to clarify that the focus of this proposed requirement would be to ensure these individuals possess these capabilities.
	(c)(5) Safeguards contingency plan.	This header would be added for formatting purposes.
§ 73.55(h)(1) Safeguards contingency plans must be in accordance with the criteria in appendix C to this part, "Licensee Safeguards Contingency Plans."	(c)(5)(i) The licensee shall establish, maintain, and implement a Commission-approved safeguards contingency plan that describes how the criteria set forth in section II of appendix C, "Licensee Safeguards Contingency Plans," to this part will be implemented.	This requirement would retain the current requirement of § 73.55(h)(1) to provide a safeguards contingency plan with minor revisions. Most significantly, the reference to appendix C to part 73 would be revised to reflect the reformatting of the proposed appendix C to part 73 which would have a section II that applies only to power reactors.
	(c)(5)(ii) The safeguards contingency plan must describe predetermined actions, plans, and strategies designed to intercept, challenge, delay, and neutralize threats up to and including the design basis threat of radiological sabotage.	This requirement would be added to generally describe the content of the Safeguards Contingency Plan.
	(c)(6) Implementing procedures.	This header would be added for formatting purposes.

§ 73.55(b)(3)(i) Written security procedures that document the structure of the security organization and detail the duties of guards, watchmen, and other individuals responsible for security.	(c)(6)(i) The licensee shall establish, maintain, and implement written procedures that document the structure of the security organization, detail the specific duties and responsibilities of each position, and implement Commission requirements through the approved security plans.	This requirement would retain the requirement for written security procedures with minor revisions. The phrase “and implement Commission requirements through the approved security plans” would be added to clarify the requirement that the licensee implements Commission requirements through procedures as well as the approved security plans.
	(c)(6)(ii) Implementing procedures need not be submitted to the Commission for prior approval, but are subject to inspection by the Commission.	This requirement would be added to address the current and proposed procedural details for implementing procedures.
	(c)(6)(iii) Implementing procedures must detail the specific actions to be taken and decisions to be made by each position of the security organization to implement the approved security plans.	This requirement would be added to describe the content of implementing procedures to clarify the current requirement "detail the duties of guards, watchmen, and other individuals responsible for security."
§ 73.55(b)(3) The licensee shall have a management system to provide for...	(c)(6)(iv) The licensee shall:	This requirement would be retained and would separate the two current requirements of § 73.55(b)(3) with minor revisions. The phrase "management system" would be replaced with the word "process." The current requirement to have a management system would be addressed in the proposed § 73.55(d)(2).

§ 73.55(b)(3) ...the development, revision, implementation, and enforcement of security procedures.	(c)(6)(iv)(A) Develop, maintain, enforce, review, and revise security implementing procedures.	This requirement would retain the requirement to develop, revise, implement, and enforce security procedures. The words “maintenance and review” would be added to clarify these tasks as necessary functions. The word “implementation” would be deleted because implementation is addressed in the proposed paragraphs (c)(6)(i) through (iii) of this section.
§ 73.55(b)(3)(ii) Provision for written approval of these procedures and any revisions to the procedures by the individual with overall responsibility for the security functions.	(c)(6)(iv)(B) Provide a process for the written approval of implementing procedures and revisions by the individual with overall responsibility for the security functions.	This requirement would retain the current requirement for written approval with minor revisions.
	(c)(6)(iv)(C) Ensure that changes made to implementing procedures do not decrease the effectiveness of any procedure to implement and satisfy Commission requirements.	This requirement would be added to ensure that the licensee process for making changes to implementing procedures includes a process to ensure that changes do not result in a reduction of effectiveness or result in a conflict with other site procedures.

	(c)(7) Plan revisions. The licensee shall revise approved security plans as necessary to ensure the effective implementation of Commission regulations and the licensee's protective strategy. Commission approval of revisions made pursuant to this paragraph is not required, provided that revisions meet the requirements of § 50.54(p) of this chapter. Changes that are beyond the scope allowed per § 50.54(p) of this chapter shall be submitted as required by §§ 50.90 of this chapter or § 73.5.	This requirement would be added to outline the three methodologies for making changes to the Commission-approved security plans and clarify that the licensee would make necessary plan changes to account for changes to site specific conditions and lessons learned from implementing the approved security plans.
§ 73.55(b) Physical Security Organization.	(d) Security organization.	This header would be retained with a minor revision.
§ 73.55(b)(1) The licensee shall establish a security organization, including guards, to protect his facility against radiological sabotage.	(d)(1) The licensee shall establish and maintain a security organization designed, staffed, trained, and equipped to provide early detection, assessment, and response to unauthorized activities within any area of the facility.	This requirement would retain the current requirement for a security organization to protect against radiological sabotage. This proposed requirement would be revised to describe a more performance based requirement consistent with the proposed paragraphs (b)(2) through (4) of this section.

		The phrase “including guards, to protect his facility against radiological sabotage” would be replaced with the phrase “designed, staffed, trained, and equipped to provide early detection, assessment, and response to unauthorized activities" to describe those elements of the security organization needed to provide the capabilities described in the proposed paragraph (b). The phrase "within any area of the facility” would be added to clarify the Commission's expectation that the licensee must implement measures consistent with site security assessments and the licensee response strategy, to facilitate the identification of a threat before an attempt to penetrate the protected area would be made.
§ 73.55(b)(3) The system shall include:	(d)(2) The security organization must include:	This requirement would be retained with minor revisions. The word “system” would be replaced by the phrase “security organization.” Although, the security “system” would include the security organization, this proposed requirement focuses only on the security organization.

§ 73.55(b)(3) The licensee shall have a management system...	(d)(2)(i) A management system that provides oversight of the onsite physical protection program.	This requirement would retain the requirement for a management system with minor revisions. Most significantly this proposed requirement would not limit the licensee management system to only provide for the development, revision, implementation, and enforcement of security procedures which are addressed in the proposed paragraph (c)(6)(iv) of this section. The Commission expectation would be that the licensee management system oversees all aspects of the onsite physical protection program to ensure the effective implementation of Commission requirements through the approved security plans and implementing procedures.
§ 73.55(b)(2) At least one full time member of the security organization who has the authority to direct the physical protection activities of the security organization shall be onsite at all times.	(d)(2)(ii) At least one member, onsite and available at all times, who has the authority to direct the activities of the security organization and who is assigned no other duties that would interfere with this individual's ability to perform these duties in accordance with the approved security plans and licensee protective strategy.	This requirement would be retained with minor revisions. The phrase “who is assigned no other duties which would interfere with” would be added to ensure that the designated individual would not be assigned any duties that would prevent or interfere with the ability to direct these activities when needed.

§ 73.55(b)(4)(i) The licensee may not permit an individual to act as a guard, watchman, armed response person, or other member of the security organization unless the individual has been trained, equipped, and qualified to perform each assigned security job duty in accordance with appendix B, "General Criteria for Security Personnel," to this part.	(d)(3) The licensee may not permit any individual to act as a member of the security organization unless the individual has been trained, equipped, and qualified to perform assigned duties and responsibilities in accordance with the requirements of appendix B to part 73 and the Commission-approved training and qualification plan.	This requirement would be retained with minor revisions.
	(d)(4) The licensee may not assign an individual to any position involving detection, assessment, or response to unauthorized activities unless that individual has satisfied the requirements of § 73.56.	This requirement would be added to clarify the prerequisite qualifications for assignment to any position involving a function upon which detection, assessment, or response capabilities depend.
§ 73.55(b)(1) If a contract guard force is utilized for site security, the licensee's written agreement with the contractor that must be retained by the licensee as a record for the duration of the contract will clearly show that:	(d)(5) If a contracted security force is used to implement the onsite physical protection program, the licensee's written agreement with the contractor must be retained by the licensee as a record for the duration of the contract and must clearly state the following conditions:	This requirement would be retained with minor revision. The phrase "utilized for site security" would be replaced with the phrase "used to implement the onsite physical protection program" to focus on the implementation of the onsite physical protection program.
§ 73.55(b)(1)(i) The licensee is responsible to the Commission for maintaining safeguards in accordance with Commission regulations and the licensee's security plan.	(d)(5)(i) The licensee is responsible for maintaining the onsite physical protection program in accordance with Commission orders, Commission regulations, and the approved security plans.	This requirement would be retained with minor revisions. Most significantly, the word "safeguards" would be replaced with the phrase" onsite physical protection program" to more accurately describe the focus of this requirement.

§ 73.55(b)(1)(ii) The NRC may inspect, copy, and take away copies of all reports and documents required to be kept by Commission regulations, orders, or applicable license conditions whether the reports and documents are kept by the licensee or the contractor.	(d)(5)(ii) The Commission may inspect, copy, retain, and remove all reports and documents required to be kept by Commission regulations, orders, or applicable license conditions whether the reports and documents are kept by the licensee or the contractor.	This requirement would be retained with minor revisions.
	(d)(5)(iii) An individual may not be assigned to any position involving detection, assessment, or response to unauthorized activities unless that individual has satisfied the requirements of § 73.56.	This requirement would be added for consistency with the proposed requirements of the proposed paragraph (d)(4) of this section. This proposed requirement would be stipulated in a contract because it relates to a function of the contract.
§ 73.55(b)(1)(iv) The contractor will not assign any personnel to the site who have not first been made aware of these responsibilities. § 73.55(b)(4)(i) The licensee may not permit an individual to act as a guard, watchman, armed response person, or other member of the security organization unless the individual has been trained, equipped, and qualified to perform each assigned security job duty in accordance with appendix B...	(d)(5)(iv) An individual may not be assigned duties and responsibilities required to implement the approved security plans or licensee protective strategy unless that individual has been properly trained, equipped, and qualified to perform their assigned duties and responsibilities in accordance with appendix B to part 73 and the Commission-approved training and qualification plan.	This requirement would retain and combine two current requirements of § 73.55(b)(1)(iv) and § 73.55(b)(4)(i) with minor revisions necessary for consistency with the proposed rule.

§ 73.55(b)(1)(iii) The requirement in paragraph (b)(4) of this section that the licensee demonstrate the ability of physical security personnel to perform their assigned duties and responsibilities, includes demonstration of the ability of the contractor's physical security personnel to perform their assigned duties and responsibilities in carrying out the provisions of the Security Plan and these regulations, and...	(d)(5)(v) Upon the request of an authorized representative of the Commission, the contractor security employees shall demonstrate the ability to perform their assigned duties and responsibilities effectively.	This requirement would be retained to describe the current requirement for demonstration by contract security personnel. The language of this current requirement would be deleted and replaced by the proposed language of the proposed § 73.55(b)(5).
	(d)(5)(vi) Any license for possession and ownership of enhanced weapons will reside with the licensee.	This requirement would be added to implement applicable portions of the EPAct 2005, and to require any security force contract to include a statement that would ensure that, all licenses relative to firearms and enhanced weapons reside with the licensee, not the contractor.
§ 73.55(c) Physical barriers.	(e) Physical barriers. Based upon the licensee's protective strategy, analyses, and site conditions that affect the use and placement of physical barriers, the licensee shall install and maintain physical barriers that are designed and constructed as necessary to deter, delay, and prevent the introduction of unauthorized personnel, vehicles, or materials into areas for which access must be controlled or restricted.	This requirement would be added to provide a performance based requirement for determining the use and placement of physical barriers required for protection of personnel, equipment, and systems, the failure of which could directly or indirectly endanger public health and safety.

		The phrase “Based upon the licensee protective strategy, analyses, and site specific conditions”, would be used to ensure that licensees consider protective strategy requirements and needs, as well as any analyses conducted by the licensee or required by the Commission to determine the effects the design basis threat could have on personnel, equipment, and systems, and any site specific condition that could have an impact on the capability to prevent significant core damage and spent fuel sabotage. The Commission considers these factors to be necessary considerations when determining the appropriate use and placement of barriers in any area.
	(e)(1) The licensee shall describe in the approved security plans, the design, construction, and function of physical barriers and barrier systems used and shall ensure that each barrier and barrier system is designed and constructed to satisfy the stated function of the barrier and barrier system.	This requirement would be added to provide a mechanism by which the licensee would confirm information regarding the use, placement, and construction of barriers, to include the intended function of specific barriers as they relate to satisfying the proposed requirements of this section.

§ 73.55(c)(9)(iii) Protect as Safeguards Information, information required by the Commission pursuant to § 73.55(c) (8) and (9). § 73.55(c)(9)(iv) Retain, in accordance with § 73.70, all comparisons and analyses prepared pursuant to § 73.55 (c)(7) and (8).	(e)(2) The licensee shall retain in accordance with § 73.70, all analyses, comparisons, and descriptions of the physical barriers and barrier systems used to satisfy the requirements of this section, and shall protect these records as safeguards information in accordance with the requirements of § 73.21.	This requirement would retain and combine the current requirements of § 73.55(c)(9)(iii) and (9)(iv) with minor revisions.
	(e)(3) Physical barriers must:	This header would be added for formatting purposes.
	(e)(3)(i) Clearly delineate the boundaries of the area(s) for which the physical barrier provides protection or a function, such as protected and vital area boundaries and stand-off distance.	This requirement would be added to provide a performance based requirement for the use of barriers.
§ 73.55(c)(8) Each licensee shall compare the vehicle control measures established in accordance with § 73.55 (c)(7) to the Commission's design goals (i.e., to protect equipment, systems, devices, or material, the failure of which could directly or indirectly endanger public health and safety by exposure to radiation) and criteria for protection against a land vehicle bomb.	(e)(3)(ii) Be designed and constructed to protect against the design basis threat commensurate to the required function of each barrier and in support of the licensee protective strategy.	This requirement would be added to apply the current requirement of § 73.55(c)(8) to compare vehicle control measures against Commission design goals, to all barriers, such as but not limited to, channeling barriers, delay barriers, and bullet resisting enclosures, and not limit this comparison to only vehicle 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.

	(e)(3)(iii) Provide visual deterrence, delay, and support access control measures.	This requirement would be added to provide a performance based requirement for physical barriers. Because of changes to the threat environment the Commission believes emphasis on the use of physical barriers would be appropriate.
	(e)(3)(iv) Support effective implementation of the licensee's protective strategy.	This requirement would be added to provide a performance based requirement for physical barriers. Because of changes to the threat environment the use of physical barriers within the licensee protective strategy would be considered essential.
	(e)(4) Owner controlled area. The licensee shall establish and maintain physical barriers in the owner controlled area to deter, delay, or prevent unauthorized access, facilitate the early detection of unauthorized activities, and control approach routes to the facility.	This requirement would be added to provide a performance based requirement to provide enhanced protection outside the protected area relative to detecting and delaying a threat before reaching any area from which the threat could disable the personnel, equipment, or systems required to meet the performance objective and requirements described in the proposed paragraph (b) of this section.
	(e)(5) Isolation zone.	This header would be added for formatting purposes.
§ 73.55(c)(3) Isolation zones shall be maintained in outdoor areas adjacent to the physical barrier at the perimeter of the protected area...	(e)(5)(i) An isolation zone must be maintained in outdoor areas adjacent to the protected area perimeter barrier. The isolation zone shall be:	This requirement would retain the current requirement for an isolation zone.

§ 73.55(c)(3) Isolation zones... and shall be of sufficient size to permit observation of the activities of people on either side of that barrier in the event of its penetration.	(e)(5)(i)(A) Designed and of sufficient size to permit unobstructed observation and assessment of activities on either side of the protected area barrier.	This requirement would retain and revise the current requirement for isolation zone design to provide observation. Most significantly, the words "designed" and "unobstructed" would be added to provide a more performance based requirement. The phrase “of people” would be deleted to focus the proposed requirement on “activities”.
§ 73.55(c)(4) Detection of penetration or attempted penetration of the protected area or the isolation zone adjacent to the protected area barrier shall assure that adequate response by the security organization can be initiated.	(e)(5)(i)(B) Equipped with intrusion detection equipment capable of detecting both attempted and actual penetration of the protected area perimeter barrier and assessment equipment capable of facilitating timely evaluation of the detected unauthorized activities before completed penetration of the protected area perimeter barrier.	This requirement would be retained and revised to require intrusion detection equipment within an isolation zone and provide a performance based requirement for that equipment. The phrase “shall assure that adequate response by the security organization can be initiated” would be moved from this proposed requirement to the proposed § 73.55(i)(9)(v).

	(e)(5)(ii) Assessment equipment in the isolation zone must provide real-time and play-back/recorded video images in a manner that allows timely evaluation of the detected unauthorized activities before and after each alarm annunciation.	This requirement would be added to provide a performance based requirement for assessment equipment utilized for the isolation zone. The Commission has determined that based on changes to threat environment the use of technology that allows for the assessment of activities before and after an alarm annunciation is necessary to facilitate a determination of the level of response needed to satisfy the performance objective and requirements of the proposed paragraph (b) of this section. The Commission believes the application of this commonly used technology would be an appropriate use of technological advancements that would effectively enhance licensee capabilities to achieve the performance objective and requirements of the proposed paragraph (b) of this section.
§ 73.55(c)(3) If parking facilities are provided for employees or visitors, they shall be located outside the isolation zone and exterior to the protected area barrier.	(e)(5)(iii) Parking facilities, storage areas, or other obstructions that could provide concealment or otherwise interfere with the licensee's capability to meet the requirements of paragraphs (e)(5)(i)(A) and (B) of this section, must be located outside of the isolation zone.	This requirement would be retained and revised to provide a performance based requirement for the areas outside the isolation zone. Most significantly, the phrase “storage areas, or other obstructions which could provide concealment or otherwise interfere” would be added to ensure that areas inside, outside, and adjacent to the protected area barrier would be maintained clear of obstructions to ensure observation and assessment capabilities.

	(e)(6) Protected area.	This header would be added for formatting purposes.
	(e)(6)(i) The protected area perimeter must be protected by physical barriers designed and constructed to meet Commission requirements and all penetrations through this barrier must be secured in a manner that prevents or delays, and detects the exploitation of any penetration.	This requirement would be added to provide a performance based requirement for physical barriers and penetrations though the protected area barrier to be secured to prevent and detect attempted or actual exploitation of the penetration. The Commission's view is that penetrations must be secured equal to the strength of the barrier of which it is a part and that attempts to exploit a penetration must be detected and response initiated.
§ 73.55(c)(2) The physical barriers at the perimeter of the protected area shall be separated from any other barrier designated as a physical barrier for a vital area within the protected area.	(e)(6)(ii) The protected area perimeter physical barriers must be separated from any other barrier designated as a vital area physical barrier, unless otherwise identified in the approved physical security plan.	This requirement would be retained with minor revision. The phrase “unless otherwise identified in the approved physical security plan” would be added to provide flexibility for an alternate methodology to be described in the Commission-approved security plans.
§ 73.55(e)(3) All emergency exits in each protected area and each vital area shall be alarmed.	(e)(6)(iii) All emergency exits in the protected area must be secured by locking devices that allow exit only and alarmed.	This requirement would retain and separate the two current requirements with minor revision. The phrase “secured by locking devices which allow exit only” would be added to provide a performance based requirement relative to the function of locking devices with emergency exit design to prevent entry. Vital areas would be addressed in the proposed § 73.55(e)(8)(vii).

	(e)(6)(iv) Where building walls, roofs, or penetrations comprise a portion of the protected area perimeter barrier, an isolation zone is not necessary, provided that the detection, assessment, observation, monitoring, and surveillance requirements of this section are met, appropriately designed and constructed barriers are installed, and the area is described in the approved security plans.	This requirement would be added to provide a performance based requirement for instances where this site condition would exist.
§ 73.55(c)(6) The walls, doors, ceiling, floor, and any windows in the walls and in the doors of the reactor control room shall be bullet-resisting. § 73.55(d)(1) The individual responsible for the last access control function (controlling admission to the protected area) must be isolated within a bullet-resisting structure as described in Paragraph (c)(6) of this section to assure his or her ability to respond or summon assistance. § 73.55(e)(1) The onsite central alarm station must be considered a vital area and its walls, doors, ceiling, floor, and any windows in the walls and in the doors must be bullet-resisting.	(e)(6)(v) The reactor control room, the central alarm station, and the location within which the last access control function for access to the protected area is performed, must be bullet-resisting.	This requirement would retain the locations identified in the current § 73.55(c)(6), (d)(1), and (e)(1). Specific reference to walls, doors, ceiling, floor, and any windows in the walls, doors, ceiling, and floor would be deleted to clarify that all construction features would be required to meet the bullet resisting requirement, and therefore remove the potential for confusion where a structural feature such as sky-lights would not be listed. The Commission does not intend to suggest that penetrations, such as heating/cooling ducts be made bullet-resistant, but rather that the licensee implement appropriate measures to prevent the exploitation of such features in a manner consistent with the intent of the bullet-resisting requirement to ensure the required functions performed in these locations are protected and maintained.

	(e)(6)(vi) All exterior areas within the protected area must be periodically checked to detect and deter unauthorized activities, personnel, vehicles, and materials.	This requirement would be added to provide a performance based requirement for monitoring exterior areas of the protected area to facilitate achievement of the requirements described by the proposed paragraph (b).
	(e)(7) Vital areas.	This header would be added for formatting purposes.
§ 73.55(c)(1) The licensee shall locate vital equipment only within a vital area, which in turn, shall be located within a protected area such that access to vital equipment requires passage through at least two physical barriers of sufficient strength to meet the performance requirements of paragraph (a) of this section.	(e)(7)(i) Vital equipment must be located only within vital areas, which in turn must be located within protected areas so that access to vital equipment requires passage through at least two physical barriers designed and constructed to perform the required function, except as otherwise approved by the Commission in accordance with paragraph (f)(2) of this section.	This requirement would be retained with minor revision. The phrase “of sufficient strength to meet the performance requirements of paragraph (a) of this section” would be replaced with the phrase “designed and constructed to perform the required function” for consistency with the proposed requirements for physical barriers discussed throughout this proposed § 73.55(e). The phrase “except as otherwise approved by the Commission in accordance with paragraph (f)(2) of this section” would be added to account for the condition addressed by paragraph (f)(2).
§ 73.55(c)(1) More than one vital area may be located within a single protected area.	(e)(7)(ii) More than one vital area may be located within a single protected area.	This requirement would be retained.

§ 73.55(e)(1) The onsite central alarm station must be considered a vital area and... § 73.55(e)(1) Onsite secondary power supply systems for alarm annunciator equipment and non-portable communications equipment as required in paragraph (f) of this section must be located within vital areas.	(e)(7)(iii) The reactor control room, the spent fuel pool, secondary power supply systems for intrusion detection and assessment equipment, non-portable communications equipment, and the central alarm station, must be provided protection equivalent to vital equipment located within a vital area.	This requirement would retain and combine two current requirements from 10 CFR 73.55(e)(1), for protecting these areas equivalent to a vital area. The Commission added the “spent fuel pool” to emphasize the Commission view that because of changes to the threat environment the spent fuel pool must also be provided this protection. The phrase “alarm annunciator” would be replaced with “intrusion detection and assessment” to clarify the application of this proposed requirement to intrusion detection sensors and video assessment equipment as well as the alarm annunciation equipment.
	(e)(7)(iv) Vital equipment that is undergoing maintenance or is out of service, or any other change to site conditions that could adversely affect plant safety or security, must be identified in accordance with § 73.58, and adjustments must be made to the site protective strategy, site procedures, and approved security plans, as necessary.	This requirement would be added to provide a performance based requirement consistent with the proposed § 73.58 Safety/Security Program.

§ 73.55(e)(3) All emergency exits in each protected area and each vital area shall be alarmed. § 73.55(d)(7)(D) Lock and protect by an activated intrusion alarm system all unoccupied vital areas.	(e)(7)(v) The licensee shall protect all vital areas, vital area access portals, and vital area emergency exits with intrusion detection equipment and locking devices. Emergency exit locking devices shall be designed to permit exit only.	This requirement would retain and combine two current requirements 10 CFR 73.55(e)(3) and (d)(7)(D) with minor revision for formatting purposes. The phrase "Emergency exit locking devices shall be designed to permit exit only" would be added to provide a performance based requirement to describe the function to be provided by emergency exit locking devices.
§ 73.55(d)(7)(D) Lock and protect by an activated intrusion alarm system all unoccupied vital areas	(e)(7)(vi) Unoccupied vital areas must be locked.	This requirement would retain the current requirement to lock unoccupied vital areas with minor revision for formatting purposes. The current requirement to alarm all vital areas would be moved to the proposed paragraph (e)(7)(v) of this section.
	(e)(8) Vehicle barrier system. The licensee must:	This header would be added for formatting purposes.
§ 73.55(c)(7) Vehicle control measures, including vehicle barrier systems, must be established to protect against use of a land vehicle, as specified by the Commission, as a means of transportation to gain unauthorized proximity to vital areas.	(e)(8)(i) Prevent unauthorized vehicle access or proximity to any area from which any vehicle, its personnel, or its contents could disable the personnel, equipment, or systems necessary to meet the performance objective and requirements described in paragraph (b) of this section.	This requirement would be retained and revised to provide a requirement for protection against any vehicle within the context of the design basis threat described in § 73.1. Because of changes to the threat environment, the meaning of the word “proximity” remains the same but is applied to include all locations from which the design basis threat could disable the personnel, equipment, or systems required to prevent radiological sabotage.

	(e)(8)(ii) Limit and control all vehicle approach routes.	This requirement would be added to provide a requirement for limiting and controlling vehicle access routes to the site for the purpose of protecting the facility against vehicle bomb attacks and the use of vehicles as a means of transporting personnel and materials that would be considered a threat. Because of changes to the threat environment the Commission has determined that control of all vehicle approach routes is a critical element of the onsite physical protection program.
	(e)(8)(iii) Design and install a vehicle barrier system, to include passive and active barriers, at a stand-off distance adequate to protect personnel, equipment, and systems against the design basis threat.	This requirement would be added to require the licensee to determine the potential effects a vehicle bomb could have on the facility and to establish a barrier system at a stand-off distance sufficient to protect personnel, equipment and systems. Because of changes to the threat environment, the Commission views stand-off distances to be a critical element of the onsite physical protection program and which require continuing analysis and evaluation to maintain effectiveness.

	(e)(8)(iv) Deter, detect, delay, or prevent vehicle use as a means of transporting unauthorized personnel or materials to gain unauthorized access beyond a vehicle barrier system, gain proximity to a protected area or vital area, or otherwise penetrate the protected area perimeter.	This requirement would be added to ensure the licensee maintains the capability to deter, detect, delay, or prevent unauthorized access beyond a vehicle barrier system. Because of changes to the threat environment, the Commission views the vehicle threat to be a critical element of the onsite physical protection program that requires continual analysis and evaluation to maintain effectiveness. This proposed requirement would include vehicles that do not reach the full capability of the design basis threat.
	(e)(8)(v) Periodically check the operation of active vehicle barriers and provide a secondary power source or a means of mechanical or manual operation, in the event of a power failure to ensure that the active barrier can be placed in the denial position within the time line required to prevent unauthorized vehicle access beyond the required standoff distance.	This requirement would be added consistent with the current requirement of § 73.55(g)(1) and would apply to the operation of active vehicle barriers within time lines required to prevent unauthorized vehicle access, despite the loss of the primary power source. The term "periodically" would be intended to allow the licensees to establish checks at a frequency necessary to ensure active barriers remain effective for both denial and non-denial operation.

	(e)(8)(vi) Provide surveillance and observation of vehicle barriers and barrier systems to detect unauthorized activities and to ensure the integrity of each vehicle barrier and barrier system.	This requirement would be added to provide a requirement for the licensee to monitor the integrity of barriers to verify availability when needed and to prevent or detect tampering. Because of changes to the threat environment, the Commission views the vehicle bomb consideration to be a critical element of the onsite physical protection program which requires continuing analysis and evaluation to maintain effectiveness.
	(e)(9) Waterways.	This header would be added for formatting purposes.
	(e)(9)(i) The licensee shall control waterway approach routes or proximity to any area from which a waterborne vehicle, its personnel, or its contents could disable the personnel, equipment, or systems necessary to meet the performance objective and requirements described in paragraph (b) of this section.	This requirement would be added to provide a requirement for controlling waterway approach routes consistent with the requirement of the proposed paragraph (e)(9)(ii) of this section. Because of changes to the threat environment, the Commission views waterway approach routes and control measures to be a critical element of the onsite physical protection program and one that requires continual analysis and evaluation to maintain effectiveness.
	(e)(9)(ii) The licensee shall delineate areas from which a waterborne vehicle must be restricted and install waterborne vehicle control measures, where applicable.	This requirement would be added to provide a requirement for notifying unauthorized individuals that access is not permitted, and the installation of barriers where appropriate.

	(e)(9)(iii) The licensee shall monitor waterway approaches and adjacent areas to ensure early detection, assessment, and response to unauthorized activity or proximity, and to ensure the integrity of installed waterborne vehicle control measures.	This requirement would be added to provide a requirement for monitoring waterway approaches consistent with other monitoring and surveillance requirements of this proposed section.
	(e)(9)(iv) Where necessary to meet the requirements of this section, licensees shall coordinate with local, state, and Federal agencies having jurisdiction over waterway approaches.	This requirement would be added to provide a requirement to coordinate where necessary with other agencies having jurisdictional authority over waterways to ensure that the proposed requirements of this section would be met.
	(e)(10) Unattended openings in any barrier established to meet the requirements of this section that are 620 cm^2 (96.1 in^2) or greater in total area and have a smallest dimension of 15 cm (5.9 in) or greater, must be secured and monitored at a frequency that would prevent exploitation of the opening consistent with the intended function of each barrier.	This requirement would be added to provide a requirement for all openings in any OCA, PA, or VA barrier to ensure that the intended function of the barrier is met. The phrase “consistent with the intended function of each barrier” would describe the criteria for making a determination to secure or monitor openings of this size where the intended function of the barrier would be compromised if the opening is not secured or monitored. The size of the opening described is a commonly accepted standard throughout the security profession for application to any security program and one that represents an opening large enough for a person to exploit.

		Therefore, the Commission has determined that openings meeting the stated criteria require measures to prevent exploitation.
	(f) Target sets.	This header would be added for formatting purposes.
	(f)(1) The licensee shall document in site procedures the process used to develop and identify target sets, to include analyses and methodologies used to determine and group the target set equipment or elements.	This requirement would be added to provide a performance based requirement for the licensee to document how each target set was developed to facilitate review of the licensee methodology by the Commission. The Commission has determined that because of changes to the threat environment the identification and protection of all target sets would be a critical component for the development and implementation of the licensee protective strategy and the capability of the licensee to prevent significant core damage and spent fuel sabotage, therefore, providing protection against radiological sabotage and satisfying the performance objective and requirements stated in the proposed paragraph (b) of this section.

	(f)(2) The licensee shall consider the effects that cyber attacks may have upon individual equipment or elements of each target set or grouping.	This requirement would be added to ensure cyber attacks associated with advancements in the area of automated computer technology are considered and the affects that such attacks may have on the integrity of individual target set equipment and elements is accounted for in the licensee protective strategy.
	(f)(3) Target set equipment or elements that are not contained within a protected or vital area must be explicitly identified in the approved security plans and protective measures for such equipment or elements must be addressed by the licensee's protective strategy in accordance with appendix C to this part.	This requirement would be added to provide a performance based requirement to identify and account for this condition in the approved security plans, if it exists at a site.
	(f)(4) The licensee shall implement a program for the oversight of plant equipment and systems documented as part of the licensee protective strategy to ensure that changes to the configuration of the identified equipment and systems do not compromise the licensee's capability to prevent significant core damage and spent fuel sabotage.	This requirement would be added to require the licensee to establish and implement a program that focuses on ensuring that certain plant equipment and systems are periodically checked to ensure that unauthorized configuration changes or tampering would be identified and an appropriate response initiated. Based on changes to the threat environment, the Commission has determined this would be an appropriate enhancement to the licensee onsite physical protection program.
	(g) Access control.	This header would be added for formatting purposes.

	(g)(1) The licensee shall:	This header would be added for formatting purposes.
§ 73.55(d)(1) The licensee shall control all points of personnel and vehicle access into a protected area.	(g)(1)(i) Control all points of personnel, vehicle, and material access into any area, or beyond any physical barrier or barrier system, established to meet the requirements of this section.	This requirement would be retained and revised with minor revisions. Most significantly, the phrase “a protected area” would be replaced by the phrase “any area, or beyond any physical barrier or barrier system, established to meet the requirements of this section” to clarify that the focus of this proposed requirement would not be limited to only protected area access but would apply to any area for which access must be controlled to meet complimentary requirements addressed in this proposed rule. In addition, the word “material’ would be added to emphasize that the control of material into these areas would also be a critical element of the onsite physical protection program to facilitate achievement of the performance objective of the proposed paragraph (b) of this section.
§ 73.55(d)(7)(i)(B) Positively control, in accordance with the access list established pursuant to paragraph (d)(7)(i) of this section, all points of personnel and vehicle access to vital areas.	(g)(1)(ii) Control all points of personnel and vehicle access into vital areas in accordance with access authorization lists.	This requirement would be retained with minor revisions.

§ 73.55(d)(7)(i) ...limit unescorted access to vital areas during nonemergency conditions to individuals who require access in order to perform their duties. To achieve this, the licensee shall:	(g)(1)(iii) During non-emergency conditions, limit unescorted access to the protected area and vital areas to only those individuals who require unescorted access to perform assigned duties and responsibilities.	This requirement would be retained and revised with minor revisions. Most significantly, the phrase “protected area” would be added to emphasize that the same “assigned duties and responsibilities” criteria apply to both vital and protected areas.
	(g)(1)(iv) Monitor and ensure the integrity of access control systems.	This requirement would be added to provide a requirement for ensuring the integrity of the access control system and prevent its unauthorized bypass. Based on changes to the threat environment, the Commission has determined that emphasis would be necessary to ensure that the integrity of the access control system is maintained through oversight and that attempts to circumvent or bypass the established process will be detected and access denied.
	(g)(1)(v) Provide supervision and control over the badging process to prevent unauthorized bypass of access control equipment located at or outside of the protected area.	This requirement would be added to provide a requirement for ensuring the integrity of the access control process. Based on changes to the threat environment, the Commission has determined that specific emphasis on access control equipment outside the protected area would be necessary to ensure that the integrity of the access control system is maintained for those process elements that are not contained within the protected area.

§ 73.55(d)(1) The individual responsible for the last access control function (controlling admission to the protected area) must be isolated within a bullet-resisting structure as described in paragraph (c)(6) of this section to assure his or her ability to respond or to summon assistance.	(g)(1)(vi) Isolate the individual responsible for the last access control function (controlling admission to the protected area) within a bullet-resisting structure to assure the ability to respond or to summon assistance in response to unauthorized activities.	This requirement would be retained and revised with minor revisions. Most significantly, the phrase “as described in paragraph (c)(6) of this section” would be deleted because the specific criteria for bullet-resisting would no longer be addressed in the referenced paragraph. Specific criteria would be addressed in standards published by the Underwriters Laboratory (UL).
	(g)(1)(vii) In response to specific threat and security information, implement a two-person (line-of-sight) rule for all personnel in vital areas so that no one individual is permitted unescorted access to vital areas. Under these conditions the licensee shall implement measures to verify that the two person rule has been met when a vital area is accessed.	This requirement would be added to require two specific actions to be taken by the licensee where credible threat information is provided. This proposed requirement would first require that the two-person rule be implemented, and second, that measures be implemented to verify that the two-person rule is met when access to a vital area is gained. This proposed requirement would include those areas identified in the proposed (e)(8)(iv) of this section to be protected as vital areas. Based on changes to the threat environment, the Commission has determined that the proposed requirement is necessary to facilitate licensee achievement of the performance objective of the proposed paragraph (b) of this section.

	(g)(2) In accordance with the approved security plans and before granting unescorted access through an access control point, the licensee shall:	This requirement would be added to specify the basic functions that must be satisfied to meet the current and proposed requirements for controlling access into any area for which access controls are implemented.
§ 73.55(d)(1) Identification...of all individuals unless otherwise provided herein must be made and...	(g)(2)(i) Confirm the identity of individuals.	This requirement would retain the current requirement with minor revisions for formatting purposes.
§ 73.55(d)(1) ...authorization must be checked at these points.	(g)(2)(ii) Verify the authorization for access of individuals, vehicles, and materials.	This requirement would retain the current requirement with minor revisions for formatting purposes.
§ 73.55(d)(1) ...search of all individuals unless otherwise provided herein must be made and...	(g)(2)(iii) Search individuals, vehicles, packages, deliveries, and materials in accordance with paragraph (h) of this section.	This requirement would retain the current requirement with minor revisions for formatting purposes.
	(g)(2)(iv) Confirm, in accordance with industry shared lists and databases, that individuals have not been denied access to another licensed facility.	This requirement would be added to describe an acceptable information sharing mechanism used by licensees to share information about visitors and employees who have requested either escorted or unescorted access to at least one site. Based on changes to the threat environment, the Commission has determined that this proposed requirement would be a prudent enhancement to the licensee capabilities.
	(g)(3) Access control points must be:	This header would be added for formatting purposes.

	(g)(3)(i) Equipped with locking devices, intrusion detection equipment, and monitoring, observation, and surveillance equipment, as appropriate.	This requirement would be added to describe the types of equipment determined to be acceptable to satisfy the desired level of performance intended by the proposed requirements of this section. The phrase "as appropriate" would be used to provide the flexibility needed to provide only that equipment that is required to accomplish the desired function of the specific access control point.
§ 73.55(d)(1) The licensee shall control all points of personnel and vehicle access into a protected area.	(g)(3)(ii) Located outside or concurrent with, the physical barrier system through which it controls access.	This requirement would be added to clarify the location of access control points to ensure personnel and vehicles do not gain access beyond a barrier (i.e., stand-off distance) before being searched.
	(g)(4) Emergency conditions.	This header would be added for formatting purposes.
§ 73.55(d)(7)(ii) Design the access authorization system to accommodate the potential need for rapid ingress or egress of individuals during emergency conditions or situations that could lead to emergency conditions. To help assure this, the licensee shall:	(g)(4)(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.	This requirement would be retained with minor revision. Most significantly, the phrase "access authorization system" would be replaced with the phrase "access control system" to clarify that the focus of this proposed requirement is on controlling access during emergency conditions. The need for rapid ingress and egress is a physical action and would more appropriately be addressed through access controls.

		Also, the phrase "authorized individuals" would be added to indicate that access authorization requirements are satisfied by the individual in advance of the need for access. In addition, the phrase “To help assure this, the licensee shall:” would be deleted because it would no longer be needed.
§ 73.55(d)(7)(ii)(A) Ensure prompt access to vital equipment.	(g)(4)(ii) Under emergency conditions, the licensee shall implement procedures to ensure that: (g)(4)(ii)(A) Authorized emergency personnel are provided prompt access to affected areas and equipment. (g)(4)(ii)(B) Attempted or actual unauthorized entry to vital equipment is detected. (g)(4)(ii)(C) The capability to prevent significant core damage and spent fuel sabotage is maintained.	This requirement would be retained and revised to add a performance based requirement that the licensee develop and maintain a process by which prompt access to vital equipment is assured while at the same time ensuring the detection of unauthorized entry, and that this process would be implemented in a manner that is consistent with the proposed requirements of this section and ensures the licensee capability to satisfy the performance objective of the proposed paragraph (b) of this section.

	(g)(4)(iii) The licensee shall ensure that restrictions for site access and egress during emergency conditions are coordinated with responses by offsite emergency support agencies identified in the site emergency plans.	This requirement would be added to provide a performance based requirement for coordination of security access controls during emergencies with the access needs of emergency response personnel. This proposed requirement is intended to provide the necessary level of flexibility to the licensee to ensure access by appropriate personnel while maintaining the necessary security posture for controlling access to areas where dangerous conditions exist, such as violent conflict involving weapons.
	(g)(5) Vehicles.	This header would be added for formatting purposes.
§ 73.55(d)(4) The licensee shall exercise positive control over all such designated vehicles to assure that they are used only by authorized persons and for authorized purposes.	(g)(5)(i) The licensee shall exercise control over all vehicles while inside the protected area and vital areas to ensure they are used only by authorized persons and for authorized purposes.	This requirement would be retained and revised to apply to all vehicles and not be limited to only designated vehicles. Most significantly, the phrase “all such designated vehicles” would be deleted to remove this limitation and clarify that the proposed requirement applies to any vehicle granted access. The word “positive” would be deleted to remove uncertainties regarding the meaning of this word.

§ 73.55(d)(4) All vehicles, except designated licensee vehicles, requiring entry into the protected area shall be escorted by a member of the security organization while within the protected area, and...	(g)(5)(ii) Vehicles inside the protected area or vital areas must be operated by an individual authorized unescorted access to the area, or must be escorted by an individual trained, qualified, and equipped to perform vehicle escort duties, while inside the area.	This requirement would be retained and would contain a significant revision to relieve the licensee from the current requirement to escort a vehicle operated by an individual who otherwise has unescorted access and relief from the requirement that a member of the security organization must escort vehicles. The phrase “escorted by a member of the security organization” would be replaced with the phrase “operated by an individual authorized unescorted access to the area, or must be escorted while inside the area” to allow personnel authorized unescorted access, to operate the vehicle without escort and to allow a vehicle to be escorted by an individual other than a member of the security organization if the operator is not authorized unescorted access. Training and qualification requirements for escorts would be addressed in the proposed § 73.55(g)(7) and (g)(8).

§ 73.55(d)(4) Designated licensee vehicles shall be limited in their use to onsite plant functions and shall remain in the protected area except for operational, maintenance, repair security and emergency purposes.	(g)(5)(iii) Vehicles inside the protected area must be limited to plant functions or emergencies, and must be disabled when not in use.	This requirement would be retained and revised. Most significantly, the phrase "Designated licensee" would be deleted to broaden the scope of this proposed requirement to all vehicles. Also, the phrase "shall remain in the protected area except for operational, maintenance, repair security and emergency purposes" would be deleted because it would no longer be needed. The word "disabled" would be added to specify that when not in use all vehicles must be rendered non-operational such that the vehicle would not be in a ready-to-use configuration.
	(g)(5)(iv) Vehicles transporting hazardous materials inside the protected area must be escorted by an armed member of the security organization.	This requirement would be added to ensure the control of hazardous material deliveries. The Commission has determined that the level of control described by this proposed requirement is prudent and necessary to satisfy the performance objective of the proposed paragraph (b) of this section.
	(g)(6) Access control devices.	This header would be added for formatting purposes.

§ 73.55(d)(5) A numbered picture badge identification system shall be used for all individuals who are authorized access to protected areas without escort.	(g)(6)(i) Identification badges. The licensee shall implement a numbered photo identification badge/key-card system for all individuals authorized unescorted access to the protected area and vital areas.	This requirement would be retained and revised with minor revisions. Most significantly, the phrase "and vital areas" is added to provide necessary focus that badges apply to both the protected area and vital areas. Access to the protected area does not include access to a vital area except as required to perform duties.
§ 73.55(d)(5)(ii) Badges may be removed from the protected area when measures are in place to confirm the true identity and authorization for access of the badge holder upon entry to the protected area.	(g)(6)(i)(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.	This requirement would be retained and revised with minor revisions. Most significantly, the phrase “upon entry to the protected area” would be replaced with the phrase “before allowing unescorted access to the protected area” to clarify that the performance to be achieved would be to confirm and verify access authorization before granting access to any individual.

§ 73.55(d)(5)(ii) Badges shall be displayed by all individuals while inside the protected area.	(g)(6)(i)(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.	This requirement would retain the current requirement to display badges at all times and would be revised to address the exception to this proposed requirement. The phrase “Except where operational safety concerns require otherwise,” would be added to account for considerations such as radiological control requirements or foreign material exclusion requirements, that may preclude this requirement. In addition, the word “clearly” would be added to describe the expected performance that badges would be visible to provide an indication of authorization to be in the area.

	(g)(6)(i)(C) The licensee shall maintain a record, to include the name and areas to which unescorted access is granted, of all individuals to whom photo identification badge/key-cards have been issued.	This requirement would be added to account for technological advancements commonly associated with electronically based badging systems used by licensees. The Commission has determined that this proposed requirement is prudent and necessary because such a record would be automatically made as a standard function and intent of this type of system. In addition, badging systems commonly used by licensees include the ability to program remote card-readers which are designed to grant or deny access to specific areas based upon the information electronically associated with specific badges/key-cards. This proposed requirement would not specify the media in which this record must be maintained to allow for electronic storage.
§ 73.55(d)(8) All keys, locks, combinations, and related access control devices used to control access to protected areas and vital areas must be controlled to reduce the probability of compromise.	(g)(6)(ii) Keys, locks, combinations, and passwords. All keys, locks, combinations, passwords, and related access control devices used to control access to protected areas, vital areas, security systems, and safeguards information must be controlled and accounted for to reduce the probability of compromise. The licensee shall:	This requirement would be retained and revised with minor revisions. Most significantly, the word “passwords” would be added to account for technological advancements associated with the use of computers. The phrase “security systems, and safeguards information” would be added to emphasize the need to control access to these items. The phrase “and accounted for” would be added to confirm possession by the individual to whom the access control device has been issued.

§ 73.55(d)(8) The licensee shall issue keys, locks, combinations, and other access control devices to protected areas and vital areas only to persons granted unescorted facility access.	(g)(6)(ii)(A) Issue access control devices only to individuals who require unescorted access to perform official duties and responsibilities.	This requirement would be retained and revised with minor revisions. Most significantly, the phrase “protected areas and vital areas” would be replaced with the phrase “to perform official duties and responsibilities” to account for access control devices to items or systems that may be located outside of protected and vital areas, such as to computer systems and safeguards information storage cabinets. The phrase “keys, locks, combinations, and other access control devices” would be replaced by the phrase "access control devices” to generically describe these items and account for other technological advancements that may occur in the future.
	(g)(6)(ii)(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.	This requirement would be added to facilitate achievement of the current requirement to control access control devices to reduce the probability of compromise. The use of key control logs and annual inventories is a commonly used mechanism for any security system and therefore, the Commission has determined that this proposed requirement is a prudent and necessary enhancement to facilitate the licensee's capability to achieve the performance objective of the proposed paragraph (b) of this section.

§ 73.55(d)(8) Whenever there is evidence or suspicion that any key, lock, combination, or related access control device may have been compromised, it must be changed or rotated.	(g)(6)(ii)(C) Implement compensatory measures upon discovery or suspicion that any access control device may have been compromised. Compensatory measures must remain in effect until the compromise is corrected.	This requirement would be retained and revised to provide a performance based requirement for compensatory measures taken in response to compromise. Most significantly, the phrase “it must be changed or rotated” would be captured in the proposed § 73.55(g)(6)(ii) (D) and (E). The phrase “Compensatory Measures must remain in effect until the compromise is corrected” would be added to provide focus specific to when compensatory measures would no longer apply.
§ 73.55(d)(8) Whenever there is evidence or suspicion that any key, lock, combination, or related access control devices may have been compromised, it must be changed or rotated.	(g)(6)(ii)(D) Retrieve, change, rotate, deactivate, or otherwise disable access control devices that have been, or may have been compromised.	This requirement would be retained and revised with minor revisions. Most significantly, the words "retrieve", "deactivate", and "disable" would be added to ensure focus is provided on these actions relative to ensuring control of access control devices and to account for electronic devices.

§ 73.55(d)(7)(C) Revoke, in the case of an individual's involuntary termination for cause, the individual's unescorted facility access and retrieve his or her identification badge and other entry devices, as applicable, prior to or simultaneously with notifying this individual of his or her termination. § 73.55(d)(8). Whenever an individual's unescorted access is revoked due to his or her lack of trustworthiness, reliability, or inadequate work performance, keys, locks, combinations, and related access control devices to which that person had access must be changed or rotated.	(g)(6)(ii)(E) Retrieve, change, rotate, deactivate, or otherwise disable all access control devices issued to individuals who no longer require unescorted access to the areas for which the devices were designed.	This requirement would retain and combine two current requirements to specify the actions required to control access control devices issued to personnel who no longer possess a need for access. The Commission has determined that the cause for revocation of unescorted access authorization does not effect the actions needed to reduce the probability of compromise. Therefore, the same actions are necessary whether access is revoked under favorable or unfavorable conditions. Whenever an individual no longer requires access to an area the access control devices issued to that individual would be retrieved, changed, rotated, deactivated, or otherwise disabled to provide high assurance that the individual would not continue to have access to the item or location.
	(g)(7) Visitors.	This header would be added for formatting purposes.

§ 73.55(d)(6) Individuals not authorized by the licensee to enter protected areas without escort shall be escorted by a watchman or other individual designated by the licensee while in a protected area and shall be badged to indicate that an escort is required.	(g)(7)(i) The licensee may permit escorted access to the protected area to individuals who do not have unescorted access authorization in accordance with the requirements of § 73.56 and part 26 of this chapter. The licensee shall:	This requirement would retain the current requirement to provide escorted access with minor revisions. This proposed requirement would address visitor access and would specify that anyone who has not satisfied the requirements of § 73.56 and part 26 of this chapter would be considered to be a visitor. The current requirement for escorts would be addressed in proposed § 73.55(g)(8).
	(g)(7)(i)(A) Implement procedures for processing, escorting, and controlling visitors.	This requirement would be added to require implementing procedures that describe how visitors would be processed, escorted, and controlled.
	(g)(7)(i)(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.	This requirement would be added to require the verification of the true identity of non-employee individuals through the presentation of photographic government issued identification (i.e., driver's license) which provides physical characteristics that can be compared to the holder. The word "recognized" would be used to provide flexibility for other types of identification that may be issued by local, state or Federal Governments.

§ 73.55(d)(6) In addition, the licensee shall require that each individual register his or her name, date, time, purpose of visit, employment affiliation, citizenship, and name of the individual to be visited.	(g)(7)(i)(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.	This requirement would be retained with minor revision.
§ 73.55(d)(6) Individuals not authorized by the licensee to enter protected areas without escort shall...be badged to indicate that an escort is required.	(g)(7)(i)(D) Issue a visitor badge to all visitors that clearly indicates that an escort is required.	This requirement would be retained with minor revision for formatting purposes. Most significantly, the word "clearly" would be added to focus on display of the badge in a manner that easily identifies the individual as requiring an escort.
§ 73.55(d)(6) Individuals not authorized by the licensee to enter protected areas without escort shall be escorted by a watchman or other individual designated by the licensee while in a protected area and	(g)(7)(i)(E) Escort all visitors, at all times, while inside the protected area and vital areas.	This requirement would retain the requirement for escort with minor revision for formatting purposes. Most significantly, the requirement for who performs these escort duties is moved to the proposed paragraph (g)(8) of this section.

§ 73.55(d)(5)(i) An individual not employed by the licensee but who requires frequent and extended access to protected and vital areas may be authorized access to such areas without escort provided that he receives a picture badge upon entrance into the protected area which must be returned upon exit from the protected area and which indicates:	(g)(7)(ii) Individuals not employed by the licensee but who require frequent and extended unescorted access to the protected area and vital areas shall satisfy the access authorization requirements of § 73.56 and part 26 of this chapter and shall be issued a non-employee photo identification badge that is easily distinguished from other identification badges before being allowed unescorted access to the protected area. Non-employee photo identification badges must indicate:	This requirement would be retained with minor revisions. Most significantly, the phrase “shall satisfy the access authorization requirements of § 73.56 and part 26 of this chapter” would be added to clarify the requirement that these individual's satisfy the same background check requirements and Behavior Observation Program participation that would be applied to any other licensee employee for unescorted access authorization. In addition, the phrase "which must be returned upon exit from the protected area" would be deleted because removal of badges from the protected area would be addressed in the proposed paragraph (g)(6)(i)(A).
§ 73.55(d)(5)(i)(A) Non-employee, no escort required;	(g)(7)(ii)(A) Non-employee, no escort required.	This requirement would be retained with minor revision for formatting purposes.
§ 73.55(d)(5)(i)(B) Areas to which access is authorized; and	(g)(7)(ii)(B) Areas to which access is authorized.	This requirement would be retained with minor revision for formatting purposes.
§ 73.55(d)(5)(i)(c) The period for which access has been authorized.	(g)(7)(ii)(C) The period for which access is authorized.	This requirement would be retained with minor revision for formatting purposes.
	(g)(7)(ii)(D) The individual's employer.	This requirement would be added to facilitate identification of this type of non-employee and the type of activities this individual should be performing.

	(g)(7)(ii)(E) A means to determine the individual's emergency plan assembly area.	This requirement would be added for emergency planning purposes.
	(g)(8) Escorts. The licensee shall ensure that all escorts are trained in accordance with appendix B to this part, the approved training and qualification plan, and licensee policies and procedures.	This requirement would be added to provided performance based requirements for satisfying the escort requirements of this proposed rule and would provide regulatory stability through the consistent application of visitor controls at all sites. Based on changes to the threat environment, the Commission has determined that emphasis on the identification and control of visitors is a prudent and necessary enhancement to facilitate licensee achievement of the performance basis of the proposed paragraph (b)(1) of this section.
	(g)(8)(i) Escorts shall be authorized unescorted access to all areas in which they will perform escort duties.	This requirement would be added to establish a basic qualification criteria for individuals performing escort duties. Individuals not authorized unescorted access to an area must be escorted and therefore, would not be qualified to perform escort duties in that area.
	(g)(8)(ii) Individuals assigned to escort visitors shall be provided a means of timely communication with both alarm stations in a manner that ensures the ability to summon assistance when needed.	This requirement would be added to establish a basic qualification criteria for individuals performing escort duties. The phrase “timely communication” would mean the ability to call for assistance before that ability can be taken away.

	(g)(8)(iii) Individuals assigned to vehicle escort duties shall be provided a means of continuous communication with both alarm stations to ensure the ability to summon assistance when needed.	This requirement would be added to establish a basic qualification criteria for individuals performing escort duties. The word “continuous communication” would mean possession of a direct line of communication for immediate notification, such as a radio.
	(g)(8)(iv) Escorts shall be knowledgeable of those activities that are authorized to be performed within the areas for which they are assigned to perform escort duties and must also be knowledgeable of those activities that are authorized to be performed by any individual for which the escort is assigned responsibility.	This requirement would be added to establish a basic qualification criteria for individuals performing escort duties. The primary responsibility of an escort would be the identification and reporting of unauthorized activities, therefore, to perform escort duties the individual must possess this knowledge in order to be an effective escort and recognize an event involving an unauthorized activity.
	(g)(8)(v) Visitor to escort ratios shall be limited to 10 to 1 in the protected area and 5 to 1 in vital areas, provided that the necessary observation and control requirements of this section can be maintained by the assigned escort over all visitor activities.	This requirement would be added to establish a basic restriction to ensure that individuals performing escort duties are able to maintain control over the personnel being escorted. The phrase "provided that the necessary observation and control requirements of this section can be maintained" would provide flexibility for the licensee to reduce the specified ratios to facilitate achievement of the performance objective of the proposed paragraph (b).
	(h) Search programs.	This header would be added for formatting purposes.

§ 73.55(d)(2) At the point of personnel and vehicle access into a protected area, all hand-carried packages shall be searched for devices such as firearms, explosives, and incendiary devices, or other items which could be used for radiological sabotage.	(h)(1) At each designated access control point into the owner controlled area and protected area, the licensee shall search individuals, vehicles, packages, deliveries, and materials in accordance with the requirements of this section and the approved security plans, before granting access.	This requirement would be retained with minor revisions. Most significantly, the phrase "for devices such as firearms, explosives, and incendiary devices, or other items which could be used for radiological sabotage" would be replaced with the phrase “in accordance with the requirements of this section and the approved security plans” to provide language that would make this proposed requirement generically applicable to all searches.
§ 73.55(d)(2) At the point of personnel and vehicle access into a protected area, all hand-carried packages shall be searched for devices such as firearms, explosives, and incendiary devices, or other items which could be used for radiological sabotage.	(h)(1)(i) The objective of the search program must be to deter, detect, and prevent the introduction of unauthorized firearms, explosives, incendiary devices, or other unauthorized materials and devices into designated areas in which the unauthorized items could be used to disable personnel, equipment, and systems necessary to meet the performance objective and requirements of paragraph (b) of this section.	This requirement would be retained and revised to focus this proposed requirement on the objective of the search program for all areas and not limit the search function to only protected and vital areas. The Commission has determined that because of changes to the threat environment, the focus of protective measures must be to protect any area from which the licensee capability to meet the performance objective and requirements of the proposed paragraph (b) of this section could be disabled or destroyed.

§ 73.55(d)(1) The search function for detection of firearms, explosives, and incendiary devices must be accomplished through the use of both firearms and explosive detection equipment capable of detecting those devices.	(h)(1)(ii) The search requirements for unauthorized firearms, explosives, incendiary devices, or other unauthorized materials and devices must be accomplished through the use of equipment capable of detecting these unauthorized items and through visual and hands-on physical searches, as needed to ensure all items are identified before granting access.	This requirement would be retained with minor revisions. The phrase “or other unauthorized materials and devices” would be added to account for future technological advancements. The phrase “and through visual and hands-on physical searches" would be added to ensure these aspects of the search process are considered and applied when needed.
	(h)(1)(iii) Only trained and qualified members of the security organization, and other trained and qualified personnel designated by the licensee, shall perform search activities or be assigned duties and responsibilities required to satisfy observation requirements for the search activities.	This requirement would be added for consistency with the current § 73.55(b)(4)(i), and clarification for “observation” of search activities by personnel. The phrase “other trained and qualified personnel designated by the licensee” would be used to account for non-security personnel who would be assigned search duties relative to supply or warehouse functions or other types of bulk shipments.
	(h)(2) The licensee shall establish and implement written search procedures for all access control points before granting access to any individual, vehicle, package, delivery, or material.	This requirement would be added for consistency with the current § 73.55(b)(3)(i).

	(h)(2)(i) Search procedures must ensure that items possessed by an individual, or contained within a vehicle or package, must be clearly identified as not being a prohibited item before granting access beyond the access control point for which the search is conducted.	This requirement would be added for consistency with the current § 73.55(d)(1) relative to the use of search equipment and to specify a requirement for the licensee to identify items that may be obscured from observation by equipment such as X-ray equipment. This requirement would ensure that human interaction with search equipment is effective and that assigned personnel are aware of all items observed or are not identified by search equipment.
	(h)(2)(ii) The licensee shall visually and physically hand search all individuals, vehicles, and packages containing items that cannot be or are not clearly identified by search equipment.	This requirement would be added for consistency with the current § 73.55(d)(1), relative to the purpose of the search function to identify items that may be obscured from observation by equipment such as X-ray equipment. This proposed requirement intends to ensure that the licensee take appropriate actions to ensure all items granted access to the PA would be identified before granting access.

§ 73.55(d)(1) Whenever firearms or explosives detection equipment at a portal is out of service or not operating satisfactorily, the licensee shall conduct a physical pat-down search of all persons who would otherwise have been subject to equipment searches.	(h)(3) Whenever search equipment is out of service or is not operating satisfactorily, trained and qualified members of the security organization shall conduct a hands-on physical search of all individuals, vehicles, packages, deliveries, and materials that would otherwise have been subject to equipment searches.	This requirement would be retained with minor revisions. The phrase “firearms or explosives detection equipment at a portal” would be replaced with the phrase “search equipment “ to generically describe this equipment. The phrase “a physical pat-down search” would be replaced with the phrase “a hands-on physical search“ to update the language commonly used to describe this activity.
§ 73.55(d)(1) When the licensee has cause to suspect that an individual is attempting to introduce firearms, explosives, or incendiary devices into protected areas, the licensee shall conduct a physical pat-down search of that individual.	(h)(4) When an attempt to introduce unauthorized items has occurred or is suspected, the licensee shall implement actions to ensure that the suspect individuals, vehicles, packages, deliveries, and materials are denied access and shall perform a visual and hands-on physical search to determine the absence or existence of a threat.	This requirement would be retained with minor revisions to provide additional performance based requirements relative to achieving the desired results.

	(h)(5) Vehicle search procedures must be performed by at least two (2) properly trained and equipped security personnel, at least one of whom is positioned to observe the search process and provide a timely response to unauthorized activities if necessary.	This requirement would be added to provide a performance based requirement for performing vehicle searches. This proposed requirement would ensure that unauthorized activities would be identified and a timely response would be initiated at a vehicle search area, to include an armed response. Based on changes to the threat environment, the Commission has determined that this requirement would facilitate achievement of the performance objective and requirements of the proposed paragraph (b) of this section.
§ 73.55(d)(4) Vehicle areas to be searched shall include the cab, engine compartment, undercarriage, and cargo area.	(h)(6) Vehicle areas to be searched must include, but are not limited to, the cab, engine compartment, undercarriage, and cargo area.	This requirement would be retained with minor revisions.
	(h)(7) Vehicle search checkpoints must be equipped with video surveillance equipment that must be monitored by an individual capable of initiating and directing a timely response to unauthorized activity.	This requirement would be added to provide additional performance based requirements relative to achieving the desired results for vehicle searches at any location designated for the performance of vehicle searches. To satisfy this proposed requirement, the individual assigned to monitor search activities need not be located in the CAS or SAS, but rather may be located in any position from which the monitoring and notification requirements of this section could be assured.

§ 73.55(d)(1) ...except bona fide Federal, State, and local law enforcement personnel on official duty to these equipment searches upon entry into a protected area. § 73.55(d)(4) ...except under emergency conditions, shall be searched for items which could be used for sabotage purposes prior to entry into the protected area.	(h)(8) Exceptions to the search requirements of this section must be submitted to the Commission for prior review and approval and must be identified in the approved security plans.	This requirement would retain, combine, and revise two current requirements § 73.55(d)(1) and (4) to generically account for those instances where search requirements would not be met before granting access beyond a physical barrier. This proposed requirement would require that the licensee specify in the approved plans the specific circumstances under which search requirements would not be satisfied.
§ 73.55(d)(3) ...except those Commission approved delivery and inspection activities specifically designated by the licensee to be carried out within vital or protected areas for reasons of safety, security or operational necessity.	(h)(8)(i) Vehicles and items that may be excepted from the search requirements of this section must be escorted by an armed individual who is trained and equipped to observe offloading and perform search activities at the final destination within the protected area.	This requirement would be retained and revised. Most significantly, this requirement would be revised to ensure that vehicles and items excepted from search requirements before entry into the protected area are escorted by an armed individual and searched when offloaded to provide assurance that unauthorized personnel and items would be detected and reported.
§ 73.55(d)(4) ...to the extent practicable, shall be off loaded in the protected area at a specific designated materials receiving area that is not adjacent to a vital area.	(h)(8)(ii) To the extent practicable, items excepted from search must be off loaded only at specified receiving areas that are not adjacent to a vital area.	This requirement would be retained with minor revision.
	(h)(8)(iii) The excepted items must be searched at the receiving area and opened at the final destination by an individual familiar with the items.	This requirement would be added to provide a performance based requirement that would ensure that the proposed requirement for search is met at the receiving area.

	§ 73.55 (i) Detection and assessment systems.	This header would be added for formatting purposes.
	(i)(1) The licensee shall establish and maintain an intrusion detection and assessment system that must provide, at all times, the capability for early detection and assessment of unauthorized persons and activities.	This requirement would be added for consistency with the current requirement of 10 CFR 73.55(e)(1) and the proposed § 73.55(b)(2) through (4). The phrase “intrusion detection and assessment system” would be intended to describe all components (i.e., personnel, procedures, and equipment) designated by the licensee as performing a function(s) required to detect or assess unauthorized activities in any area to which access must be controlled to meet Commission requirements. The term "system" refers to how these components interact to satisfy Commission requirements. This proposed requirement does not mandate specific intrusion detection equipment for any specific area, but rather requires that the system provide detection and assessment capabilities that meet Commission requirements. The phrase "at all times" is used to describe the Commission's view that the licensee must have in place and operational a mechanism by which all threats will be detected and an appropriate response initiated, at any time.

		The Commission does not mean to suggest that a failure of any component of a system would constitute an automatic non-compliance with this proposed requirement provided the failure is identified and compensatory measures are implemented within a time frame consistent with the time lines necessary to prevent exploitation of the failure, beginning at the time of the failure.
§ 73.55(e)(1) All alarms required pursuant to this part must annunciate in a continuously manned central alarm station located within the protected area and in at least one other continuously manned station not necessarily onsite, so that a single act cannot remove the capability of calling for assistance or otherwise responding to an alarm.	(i)(2) Intrusion detection equipment must annunciate, and video assessment equipment images shall display, concurrently in at least two continuously staffed onsite alarm stations, at least one of which must be protected in accordance with the requirements of paragraphs (e)(6)(v), (e)(7)(iii), and (i)(8)(ii) of this section.	This requirement would be retained with three significant revisions. The most significant revision would be the deletion of the current language that describes where the secondary alarm station may be located. Because of changes to the threat environment the Commission has determined that to ensure the functions required to be performed by the central alarm are maintained, both alarm stations must be located onsite. As all current licensees have their secondary alarm station onsite, the Commission has determined that deletion of the "not necessarily onsite" provision, would have no impact.

		The second significant revision is the addition of the word "concurrently" to provide a performance based requirement that focuses on the need to ensure that both alarm station operators are notified of a potential threat, are capable of making a timely and independent assessment, and have equal capabilities to ensure that a timely response is made. This proposed requirement would be necessary for consistency with the current requirement to protect against a single act. The third significant revision would be the addition of the phrase “and video assessment equipment images shall display” to add a performance based requirement that focuses on the relationship between detection and assessment.
	(i)(3) The licensee's intrusion detection system must be designed to ensure that both alarm station operators: (i)(3)(i) Are concurrently notified of the alarm annunciation. (i)(3)(ii) Are capable of making a timely assessment of the cause of each alarm annunciation. (i)(3)(iii) Possess the capability to initiate a timely response in accordance with the approved security plans, licensee protective strategy, and implementing procedures.	This requirement would be added to provide performance based requirements consistent with the current § 73.55(e)(1), and the proposed requirements of this proposed section. The proposed requirement for dual knowledge and dual capability within both alarm stations provides a defense-in-depth component consistent with the proposed requirement for protection against a single act.

		Based on changes to the threat environment the Commission has determined this proposed requirement is a prudent clarification of current requirements necessary to facilitate the licensee capability to achieve the performance objective of the proposed paragraph (b)(1) of this section.
	(i)(4) Both alarm stations must be equipped with equivalent capabilities for detection and communication, and must be equipped with functionally equivalent assessment, monitoring, observation, and surveillance capabilities to support the effective implementation of the approved security plans and the licensee protective strategy in the event that either alarm station is disabled.	This requirement would be added for consistency with the current § 73.55(e)(1) and the proposed requirements for defense-in-depth and protection against a single act. The word "equivalent" would require the licensee to provide both alarm stations with detection and communication equipment that ensures each alarm station operator is knowledgeable of an alarm annunciation at each alarm point and zone, and can communicate the initiation of an appropriate response to include the disposition of each alarm. The phrase "functionally equivalent" would require that both alarm stations be equally equipped to perform those assessment, surveillance, observation, and monitoring functions needed to support the effective implementation of the licensee protective strategy.

		This proposed requirement would clarify the Commission expectation that those video technologies and capabilities used to support the effective implementation of the approved security plans and the licensee protective strategy are equally available for use by both alarm station operators to ensure that the functions of detection, assessment, and communications can be effectively maintained and utilized in the event that one or the other alarm station is disabled. Based on changes to the threat environment the Commission has determined that this proposed requirement is a prudent and necessary clarification of current requirements and Commission Orders necessary to ensure the performance objective and requirements of the proposed paragraph (b) of this section are met.
§ 73.55(e)(1) ...so that a single act cannot remove the capability of calling for assistance or otherwise responding to an alarm.	(i)(4)(i) The licensee shall ensure that a single act cannot remove the capability of both alarm stations to detect and assess unauthorized activities, respond to an alarm, summon offsite assistance, implement the protective strategy, provide command and control, or otherwise prevent significant core damage and spent fuel sabotage.	This requirement would be retained and revised to provide additional clarification regarding the critical functions determined essential and which must be maintained to carry out an effective response to threats consistent with the proposed performance objective and requirements of paragraph (b) of this section.

§ 73.55(e)(1) Onsite secondary power supply systems for alarm annunciator equipment ...	(i)(4)(ii) The alarm station functions in paragraph (i)(4) of this section must remain operable from an uninterruptible backup power supply in the event of the loss of normal power.	This requirement would retain the current requirement for secondary power with two significant revisions. First, the phrase "annunciator equipment" would be replaced with the phrase "alarm station functions" to ensure that the equipment required by each alarm station to fulfill its assigned functions, are available and operational without interruption due to a loss of normal power. Second, the word “uninterruptible” would be added to clarify the Commission's view that the operation of detection and assessment equipment must be maintained without interruption, in the event of a loss of normal power. Backup power supply for non-portable communication equipment is addressed in the proposed paragraph (j)(5) of this section. Based on changes to the threat environment, the Commission has determined that this proposed requirement is prudent and necessary to facilitate achievement of the performance objective and requirements of the proposed paragraph (b) of this section.

	(i)(5) Detection. Detection capabilities must be provided by security organization personnel and intrusion detection equipment, and shall be defined in implementing procedures. Intrusion detection equipment must be capable of operating as intended under the conditions encountered at the facility.	This requirement would be added for consistency with the current § 73.55(c)(4) and to provide a performance based requirement for detection equipment to be capable of operating under known/normal site conditions such as heat, wind, humidity, fog, cold, snowfall, etc. Equipment failure and abnormal or severe weather cannot always be predicted but compensatory measures would be required in accordance with the proposed requirements of this section to ensure compliance.
	(i)(6) Assessment. Assessment capabilities must be provided by security organization personnel and video assessment equipment, and shall be described in implementing procedures. Video assessment equipment must be capable of operating as intended under the conditions encountered at the facility and must provide video images from which accurate and timely assessments can be made in response to an alarm annunciation or other notification of unauthorized activity.	This requirement would be added for consistency with the current § 73.55(c)(4) and to provide a performance based requirement for assessment equipment to be capable of operating under known/normal site conditions such as heat, wind, humidity, fog, cold, snowfall, etc. Equipment failure and abnormal or severe weather cannot always be predicted but compensatory measures would be required in accordance with the proposed requirements of this section to ensure compliance.
	(i)(7) The licensee intrusion detection and assessment system must:	This requirement would be added for formatting purposes.

	(i)(7)(i) Ensure that the duties and responsibilities assigned to personnel, the use of equipment, and the implementation of procedures provides the detection and assessment capabilities necessary to meet the requirements of paragraph (b) of this section.	This requirement would be added to provide a performance based requirement relative to the design of the licensee detection and assessment system and to clarify that this system would include all three components.
§ 73.55(e)(2) The annunciation of an alarm at the alarm stations shall indicate the type of alarm (e.g., intrusion alarms, emergency exit alarm, etc.) and location.	(i)(7)(ii) Ensure that annunciation of an alarm indicates the type and location of the alarm.	This requirement would be retained with minor revision. The phrase “at the alarm stations” and the listed examples would be deleted because they would no longer be needed.
§ 73.55(e)(2) All alarm devices including transmission lines to annunciators shall be tamper indicating and self-checking .	(i)(7)(iii) Ensure that alarm devices, to include transmission lines to annunciators, are tamper indicating and self-checking.	This requirement would be retained with minor revision for formatting purposes.
	(i)(7)(iv) Provide visual and audible alarm annunciation and concurrent video assessment capability to both alarm stations in a manner that ensures timely recognition, acknowledgment and response by each alarm station operator in accordance with written response procedures.	This requirement would be added for consistency with the proposed requirement for equivalent capabilities in both alarm stations. The phrase “visual and audible” would provide redundancy to ensure that each alarm would be recognized and acknowledged when received.
§ 73.55(e)(2) ...e.g., an automatic indication is provided when failure of the alarm system or a component occurs, or when the system is on standby power.	(i)(7)(v) Provide an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply.	This requirement would be retained with minor revision for formatting purposes.

§ 73.70(f) A record at each onsite alarm annunciation location of each alarm, false alarm, alarm check, and tamper indication that identifies the type of alarm, location, circuit, date, and time. In addition, details of response by facility guards and watchmen to each alarm, intrusion, or other incident shall be recorded.	(i)(7)(vi) Maintain a record of all alarm annunciations, the cause of each alarm, and the disposition of each alarm.	This requirement would be added for consistency with § 73.70(f). The Commission expects that this record would be a commonly maintained record in electronic form which is generated as an automatic function of the intrusion detection system.
	(i)(8) Alarm stations.	This header would be added for formatting purposes.
§ 73.55(e)(1) All alarms required pursuant to this part must annunciate in a continuously manned central alarm station located within the protected area and in at least one other continuously manned station...	(i)(8)(i) Both alarm stations must be continuously staffed by at least one trained and qualified member of the security organization.	This requirement would retain the current requirement § 73.55(e)(1) for continuously staffed alarm stations and would be revised to describe the necessary qualifications that would be required of the assigned individuals.
§ 73.55(e)(1) The onsite central alarm station must be located within a building in such a manner that the interior of the central alarm station is not visible from the perimeter of the protected area.	(i)(8)(ii) The interior of the central alarm station must not be visible from the perimeter of the protected area.	This requirement would be retained with minor revision. Most significantly, the phrase "located within a building" would be deleted because it would be considered unnecessary.
§ 73.55(e)(1) This station must not contain any operational activities that would interfere with the execution of the alarm response function.	(i)(8)(iii) The licensee may not permit any activities to be performed within either alarm station that would interfere with an alarm station operator's ability to effectively execute assigned detection, assessment, surveillance, and communication duties and responsibilities.	This requirement would be retained with minor revisions to provide a performance based requirement regarding the primary duties required to satisfy the current requirement "execution of the alarm response function."

	(i)(8)(iv) The licensee shall assess and respond to all alarms and other indications of unauthorized activities in accordance with the approved security plans and implementing procedures.	This requirement would be added for consistency with current requirements. The specific requirements of the current § 73.55(h)(4) are retained in detail in the proposed appendix C to part 73.
	(i)(8)(v) The licensee implementing procedures must ensure that both alarm station operators are knowledgeable of all alarm annunciations, assessments, and final disposition of all alarms, to include but not limited to a prohibition from changing the status of a detection point or deactivating a locking or access control device at a protected or vital area portal, without the knowledge and concurrence of the other alarm station operator.	This requirement would be added for consistency with related requirements of this proposed section and to ensure that the licensee provides a process by which both alarm station operators are concurrently made aware of each alarm and are knowledgeable of how each alarm is resolved and that no one alarm station operator can manipulate alarm station equipment, communications, or procedures without the knowledge and concurrence of the other.
	(i)(9) Surveillance, observation, and monitoring.	This header would be added for formatting purposes.
	(i)(9)(i) The onsite physical protection program must include the capability for surveillance, observation, and monitoring in a manner that provides early detection and assessment of unauthorized activities.	This requirement would be added to provide a performance based requirement for ensuring surveillance, observation, and monitoring capabilities in any area for which these measures are necessary to meet the requirements of this proposed section.

	(i)(9)(ii) The licensee shall provide continual surveillance, observation, and monitoring of all areas identified in the approved security plans as requiring surveillance, observation, and monitoring to ensure early detection of unauthorized activities and to ensure the integrity of physical barriers or other components of the onsite physical protection program.	This requirement would be added to provide a performance based requirement for ensuring surveillance, observation, and monitoring capabilities in any area for which these measures are necessary to meet the requirements of this proposed section. The word “continual” would mean regularly recurring actions such that designated areas would be checked at intervals sufficient to ensure the detection of unauthorized activities.
	(i)(9)(ii)(A) Continual surveillance, observation, and monitoring responsibilities must be performed by security personnel during routine patrols or by other trained and equipped personnel designated as a component of the protective strategy.	This requirement would be added to provide necessary qualifying requirements for performance of observation and monitoring activities. The word “continual” would mean the same as used in the proposed paragraph (i)(9)(ii) of this section.
	(i)(9)(ii)(B) Surveillance, observation, and monitoring requirements may be accomplished by direct observation or video technology.	This requirement would be added to provide a performance based requirement for ensuring that surveillance, observation, and monitoring capabilities that may be met through the use of video technology or direct human observation.

	(i)(9)(iii) The licensee shall provide random patrols of all accessible areas containing target set equipment.	This requirement would be added to focus a performance based requirement on the protection of target set equipment. Target set equipment would be addressed in detail in the proposed paragraph (f) of this section. The term “random” provides flexibility to the licensee and requires patrols at unpredictable times within predetermined intervals to deter exploitation of periods between patrols. The phrase “accessible areas” would exclude areas such as locked high radiation areas or other such areas containing a significant safety concern that would preclude the conduct of the patrol function.
	(i)(9)(iii)(A) Armed security patrols shall periodically check designated areas and shall inspect vital area entrances, portals, and external barriers.	This requirement would be added to focus on the items that, because of changes to the threat environment, the Commission has determined would require focus by armed security patrols. The term “periodically” provides flexibility to the licensee. The phrase "designated areas" means any area identified by the licensee as requiring an action to meet the proposed requirements of this section.

	(i)(9)(iii)(B) Physical barriers must be inspected at random intervals to identify tampering and degradation.	This requirement would be added for consistency with the current requirement § 73.55(g)(1) and to focus on verifying the integrity of physical barriers to ensure that the barrier would perform as expected. The word "random" would mean that the required inspection would be performed at unpredictable times to deter exploitation of periods between inspections.
§ 73.55(b)(4)(i) The licensee may not permit an individual to act as a guard, watchman, armed response person, or other member of the security organization unless the individual has been trained, equipped, and qualified to perform each assigned security job duty.	(i)(9)(iii)(C) Security personnel shall be trained to recognize indications of tampering as necessary to perform assigned duties and responsibilities as they relate to safety and security systems and equipment.	This requirement would be added for consistency with the current requirement § 73.55(b)(4)(i) to provide necessary focus on the threat of tampering and the need to ensure that personnel are trained to recognize it.
	(i)(9)(iv) Unattended openings that are not monitored by intrusion detection equipment must be observed by security personnel at a frequency that would prevent exploitation of that opening.	This requirement would be added to provide a performance based requirement to ensure that unattended openings that cross a security boundary established to meet the proposed requirements of this section would not be exploited by the design basis threat of radiological sabotage to include the use of tools to enlarge the opening.

§ 73.55(h)(4) Upon detection of abnormal presence or activity of persons or vehicles..., the licensee security organization shall...	(i)(9)(v) Upon detection of unauthorized activities, tampering, or other threats, the licensee shall initiate actions consistent with the approved security plans, the licensee protective strategy, and implementing procedures.	This requirement would be retained with minor revision to provide flexibility for the licensee to determine if all or only part of the protective strategy capabilities would be needed for a specific event. The phrase "abnormal presence or activity of persons or vehicles" would be replaced with the phrase "unauthorized activities, tampering, or other threats" to clarify the types of activities that would be expected to warrant a response by the licensee.
	(i)(10) Video technology.	This header would be added for formatting purposes.
	(i)(10)(i) The licensee shall maintain in operable condition all video technology used to satisfy the monitoring, observation, surveillance, and assessment requirements of this section.	This requirement would be added for consistency with the current requirement § 73.55(g)(1) and would provide a performance based requirement for ensuring video technology is operating and available when needed.
	(i)(10)(ii) Video technology must be:	This header would be added for formatting purposes.
	(i)(10)(ii)(A) Displayed concurrently at both alarm stations.	This requirement would be added for consistency with the other proposed requirements for dual alarm stations and would focus on the need for video technology to be provided to both alarm stations at the same time to ensure that an assessment would be made and a timely response would be initiated.

	(i)(10)(ii)(B) Designed to provide concurrent observation, monitoring, and surveillance of designated areas from which an alarm annunciation or a notification of unauthorized activity is received.	This requirement would be added for consistency with the other proposed requirements for dual alarm stations and would focus on the need for the same capabilities to be provided to both to ensure observation, monitoring, and surveillance requirements are met.
	(i)(10)(ii)(C) Capable of providing a timely visual display from which positive recognition and assessment of the detected activity can be made and a timely response initiated.	This requirement would be added to provide a performance based requirement for video technology which focuses on the need for clear visual images from which accurate and timely assessment can be made in response to alarm annunciations.
§ 73.55(h)(6) To facilitate initial response to detection of penetration ...preferably by means of closed circuit television or by other suitable means which limit exposure of responding personnel to possible attack.	(i)(10)(ii)(D) Used to supplement and limit the exposure of security personnel to possible attack.	This requirement would retain the current requirement to use video technology to limit the exposure of security personnel while performing security duties with minor revision to add patrols.

	(i)(10)(iii) The licensee shall implement controls for personnel assigned to monitor video technology to ensure that assigned personnel maintain the level of alertness required to effectively perform the assigned duties and responsibilities.	This requirement would be added to provide a performance based requirement relative to controlling personnel fatigue related to extended periods of monitoring video technology. The Commission has determined that each individual's alertness is critical to the effective use of video technology and the licensee capability to achieve the performance objective of this proposed section. Therefore, licensee work hour controls should ensure that assigned personnel are relieved of these duties and assigned other duties at intervals sufficient to ensure the individual's ability to effectively carry out assigned duties and responsibilities.
	(i)(11) Illumination.	This header would be added for formatting purposes.

§ 73.55(c)(5) Isolation zones and all exterior areas within the protected area shall be provided with illumination sufficient for the monitoring and observation requirements of paragraphs (c)(3), (c)(4), and (h)(4) of this section, but...	(i)(11)(i) The licensee shall ensure that all areas of the facility, to include appropriate portions of the owner controlled area, are provided with illumination necessary to satisfy the requirements of this section.	This requirement would be retained and revised. Most significantly, this proposed requirement would expand a performance based lighting requirement to all areas designated by the licensee as having a need for detection, assessment, surveillance, observation, and monitoring, capabilities in support of the protective strategy and not limit it to only the isolation zone and all exterior areas within the protected area. This requirement would not require deterministic illumination levels but rather would require that illumination levels be sufficient to provide the detection, assessment, surveillance, observation, and monitoring, capabilities described by the licensee in the approved security plans. This description would be required to consider the requirements of the proposed (i)(11)(ii) and (iii).

§ 73.55(c)(5) Isolation zones and all exterior areas within the protected area shall be provided with illumination ...not less than 0.2 footcandle measured horizontally at ground level.	(i)(11)(ii) The licensee shall provide a minimum illumination level of 0.2 footcandle measured horizontally at ground level, in the isolation zones and all exterior areas within the protected area, or may augment the facility illumination system, to include patrols, responders, and video technology, with low-light technology capable of meeting the detection, assessment, surveillance, observation, monitoring, and response requirements of this section.	This requirement would be retained and revised to provide a performance based requirement for illumination. Most significantly, this proposed requirement would maintain the current 0.2 footcandle lighting requirement but would also provide flexibility to a licensee to provide less than the 0.2 footcandle where low-light technology would be used to maintain the capability to meet the performance level for detection, assessment, surveillance, observation, monitoring, and response. The word "or" would be used specifically to mean that the licensee need satisfy only one of the two options such that the 0.2 footcandle requirement must be met in the isolation zone and all exterior areas within the protected area unless low-light technology is used. However, the word "augment" would be used to represent the Commission's view that sole use of low-light technology is not authorized as this approach would be contrary to defense-in-depth and could be susceptible to single failure where a counter technology is developed or used.
	(i)(11)(iii) The licensee shall describe in the approved security plans how the lighting requirements of this section are met and, if used, the type(s) and application of low-light technology used.	This requirement would be added to clarify the need for lighting to be described in the approved security plans and how the lighting "system" would be used to achieve the performance objective.

73.55(f) Communication requirements.	(j) Communication requirements.	This header would be retained. The current requirements under this header are retained and reformatted to individually address each current requirement. Significant revisions would be specifically identified as each current requirement is addressed.
§ 73.55(f)(1) Each guard, watchman or armed response individual on duty shall be capable of maintaining continuous communication with an individual in each continuously manned alarm station required by paragraph (e)(1) of this section...	(j)(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.	This requirement would be retained with minor revision. Most significantly, the specific language of the current requirement would be revised to a more performance based requirement. The word "continuous" would be used to mean that a communication method would be available and operating any time it would be needed to communicate information.
§ 73.55(f)(1) ...who shall be capable of calling for assistance from other guards, watchmen, and armed response personnel and from local law enforcement authorities.	(j)(2) Individuals assigned to each alarm station shall be capable of calling for assistance in accordance with the approved security plans, licensee integrated response plan, and licensee procedures.	This requirement would be retained with minor revision. Most significantly, in order to provide flexibility and to capture the proposed requirements of appendix C to part 73 for an Integrated Response Plan, this proposed requirement replaces the specific list of support entities to be called with a performance based requirement to follow predetermined actions.

§ 73.55(f)(1) Each guard, watchman or armed response individual on duty shall be capable of maintaining continuous communication with an individual in each continuously manned alarm station required by paragraph (e)(1) of this section...	(j)(3) Each on-duty security officer, watchperson, vehicle escort, and armed response force member shall be capable of maintaining continuous communication with an individual in each alarm station.	This requirement would be retained with minor revisions. Most significantly, this proposed requirement would update the titles used to identify the listed positions and would add "vehicle escorts" for consistency with the proposed paragraph (g)(8) of this section.
§ 73.55(f)(3) To provide the capability of continuous communication... and shall terminate in each continuously manned alarm station required by paragraph (e)(1) of this section.	(j)(4) The following continuous communication capabilities must terminate in both alarm stations required by this section:	This requirement would be retained with minor revision for formatting purposes.
§ 73.55(f)(2) The alarm stations required by paragraph (e)(1) of this section shall have conventional telephone service for communication with the law enforcement authorities as described in paragraph (f)(1) of this section.	(j)(4)(i) Conventional telephone service.	This requirement would be retained with minor revision. Most significantly, the phrase "with the law enforcement authorities as described in paragraph (f)(1) of this section" would be deleted because site plans and procedures would contain protocols for contacting support personnel and agencies.
§ 73.55(f)(3) To provide the capability of continuous communication, radio or microwave transmitted two-way voice communication, either directly or through an intermediary, shall be established, in addition to conventional telephone service, between local law enforcement authorities and the facility and...	(j)(4)(ii) Radio or microwave transmitted two-way voice communication, either directly or through an intermediary.	This requirement would be retained with minor revision. Most significantly, the phrase "shall be established, in addition to conventional telephone service, between local law enforcement authorities and the facility and" would be deleted because site plans and procedures would contain protocols for contacting support personnel and agencies.

	(j)(4)(iii) A system for communication with all control rooms, on-duty operations personnel, escorts, local, state, and Federal law enforcement agencies, and all other personnel necessary to coordinate both onsite and offsite responses.	This requirement would be added for consistency with the proposed requirements of this section and to provide a performance based requirement for communications consistent with the proposed Integrated Response Plan addressed in the proposed appendix C to part 73.
§ 73.55(f)(4) Non-portable communications equipment controlled by the licensee and required by this section shall remain operable from independent power sources in the event of the loss of normal power.	(j)(5) Non-portable communications equipment must remain operable from independent power sources in the event of the loss of normal power.	This requirement would be retained with minor revision. Most significantly, the phrase “controlled by the licensee and required by this section” would be deleted because there would be no requirement for non-portable communications equipment that is not under licensee control or not required by this section.
	(j)(6) The licensee shall identify site areas where communication could be interrupted or can not be maintained and shall establish alternative communication measures for these areas in implementing procedures.	This requirement would be added to ensure the capability to communicate during both normal and emergency conditions, and to focus attention on the requirement that the licensee must identify site areas in which communications could be lost and account for those areas in their procedures.
73.55(h) Response requirement.	(k) Response requirements.	This header would be retained.
	(k)(1) Personnel and equipment.	This header would be added for formatting purposes.

	(k)(1)(i) The licensee shall establish and maintain, at all times, the minimum number of properly trained and equipped personnel required to intercept, challenge, delay, and neutralize threats up to and including the design basis threat of radiological sabotage as defined in § 73.1, to prevent significant core damage and spent fuel sabotage.	This requirement would be added to provide a performance based requirement for determining the minimum number of armed responders needed to protect the facility against the full capability of the design basis threat. The phrase "to intercept, challenge, delay, and neutralize threats up to and including the design basis threat of radiological sabotage as defined in § 73.1, to prevent significant core damage and spent fuel sabotage" would be used for consistency with the proposed paragraphs (b)(2) through (4) of this section.
	(k)(1)(ii) The licensee shall provide and maintain firearms, ammunition, and equipment capable of performing functions commensurate to the needs of each armed member of the security organization to carry out their assigned duties and responsibilities in accordance with the approved security plans, the licensee protective strategy, implementing procedures, and the site specific conditions under which the firearms, ammunition, and equipment will be used.	This requirement would be added to provide a performance based requirement to ensure that the licensee provides weapons that are capable of performing the functions required for each armed individual to fulfill their assigned duties per the licensee protective strategy. For example, if an individual is assigned to a position for which the protective strategy requires weapons use at 200 meters, then the assigned weapon must be capable of that performance as well as the individual.

	(k)(1)(iii) The licensee shall describe in the approved security plans, all firearms and equipment to be possessed by and readily available to, armed personnel to implement the protective strategy and carry out all assigned duties and responsibilities. This description must include the general distribution and assignment of firearms, ammunition, body armor, and other equipment used.	This requirement would be added to ensure that the licensee provides, in the approved security plans, a description of the weapons to be used and those equipment designated as readily available.
	(k)(1)(iv) The licensee shall ensure that all firearms, ammunition, and equipment required by the protective strategy are in sufficient supply, are in working condition, and are readily available for use in accordance with the licensee protective strategy and predetermined time lines.	This requirement would be added to provide a performance based requirement to ensure the availability and operability of equipment needed to accomplish response goals and objectives during postulated events. The term “readily available” would mean that required firearms and equipment are either in the individuals possession or at pre-staged locations such that required response time lines are met.

	(k)(1)(v) The licensee shall ensure that all armed members of the security organization are trained in the proper use and maintenance of assigned weapons and equipment in accordance with appendix B to part 73.	This requirement would be added to provide a performance based requirement to ensure that all armed personnel meet standard training program requirements and specific training requirements applicable to the specific weapons they are assigned, to include the maintenance required for each to ensure operability. The ability for armed personnel to trouble-shoot a problem, such as a jammed round during an actual event, would be considered a critical function necessary to achieve the performance objective.
§ 73.55(h)(5) The licensee shall instruct every guard and all armed response personnel to prevent or impede attempted acts of theft or radiological sabotage by using force sufficient to counter the force directed at him including the use of deadly force when the guard or other armed response person has a reasonable belief it is necessary in self-defense or in the defense of others.	(k)(2) The licensee shall instruct each armed response person to prevent or impede attempted acts of theft or radiological sabotage by using force sufficient to counter the force directed at that person including the use of deadly force when the armed response person has a reasonable belief that the use of deadly force is necessary in self-defense or in the defense of others, or any other circumstances as authorized by applicable state law.	This requirement would be retained with some revision. The term "guard" was removed as the term is no longer used. The phrase "or any other circumstances as authorized by applicable state law" would be added to clarify that applicable state law specifies the conditions under which deadly force may be applied. It is important to note that the use of deadly force should be a last resort when all other lesser measures to neutralize the threat have failed. The conditions under which deadly force would be authorized are governed by State laws and nothing in this proposed rule should be interpreted to mean or require anything that would contradict such state law. The term "it" is replaced with the phrase "deadly force" to more clearly describe the action.

	(k)(3) The licensee shall provide an armed response team consisting of both armed responders and armed security officers to carry out response duties, within predetermined time lines.	This requirement would be added to provide a performance based requirement that would retain the current requirement for armed responders and add a category of armed security officer to clarify the division of types of armed response personnel and their roles.
	(k)(3)(i) Armed responders.	This header would be added for formatting purposes.
§ 73.55(h)(3) The total number of guards, and armed, trained personnel immediately available at the facility to fulfill these response requirements shall nominally be ten (10), unless specifically required otherwise on a case by case basis by the Commission; however, this number may not be reduced to less than five (5) guards.	(k)(3)(i)(A) The licensee shall determine the minimum number of armed responders necessary to protect against the design basis threat described in § 73.1(a), subject to Commission approval, and shall document this number in the approved security plans.	This requirement would be retained and revised to remove the specific minimum numbers of 10, but no less than 5, to provide a performance based requirement that meets the proposed requirement of paragraph (k)(1)(i) of this section. This proposed requirement would ensure that the licensee would provide the requisite number of armed responders needed to carry-out the protective strategy, the effectiveness of which would be evaluated through annual exercises and triennial exercises observed by the Commission.
§ 73.55(h)(3) The total number of guards, and armed, trained personnel immediately available at the facility to fulfill these response requirements...	(k)(3)(i)(B) Armed responders shall be available at all times inside the protected area and may not be assigned any other duties or responsibilities that could interfere with assigned response duties.	This requirement would be retained and revised. Most significantly, this proposed requirement would specify the conditions that must be met to satisfy the meaning of the word "available" as used.
	(k)(3)(ii) Armed security officers.	This header would be added for formatting purposes.

	(k)(3)(ii)(A) Armed security officers designated to strengthen response capabilities shall be onsite and available at all times to carry out assigned response duties.	This requirement would be added to provide a performance based requirement for the licensee to identify a new category of armed personnel to be used to supplement and support the armed responders identified in the proposed paragraph (k)(3)(ii)(A) of this section.
§ 73.55(h)(3) The total number of guards, and armed, trained personnel immediately available at the facility to fulfill these response requirements shall nominally be ...	(k)(3)(ii)(B) The minimum number of armed security officers must be documented in the approved security plans.	This requirement would be added to require licensees to document the number of armed security officers to be used.
	(k)(3)((iii) The licensee shall ensure that training and qualification requirements accurately reflect the duties and responsibilities to be performed.	This requirement would be added for consistency with the current requirement § 73.55(b)(4)(ii) for an approved T&Q plan and the current requirement for licensees to document how these personnel are to be trained and qualified.
	(k)(3)(iv) The licensee shall ensure that all firearms, ammunition, and equipment needed for completing the actions described in the approved security plans and licensee protective strategy are readily available and in working condition.	This requirement would be added for consistency with the current § 73.55(g)(1) to ensure that all firearms and equipment required by each member of the armed response team would be operable and in the possession of or available at pre-staged locations, to ensure that each individual is able to meet the time lines specified by the protective strategy. This includes those equipment designated as readily available.

	(k)(4) The licensee shall describe in the approved security plans, procedures for responding to an unplanned incident that reduces the number of available armed response team members below the minimum number documented by the licensee in the approved security plans.	This requirement would be added to provide regulatory consistency for the period of time a licensee may not meet the minimum numbers stated in the approved plans because of illness or injury to an assigned individual or individuals while on-duty.
	(k)(5) Protective Strategy. Licensees shall develop, maintain, and implement a written protective strategy in accordance with the requirements of this section and appendix C to this part.	This requirement would be added to provide a performance based requirement for the development of a protective strategy that specifies how the licensee will utilize onsite and offsite, the resources to ensure the performance objective of how the proposed paragraph (b) of this section is met.
	(k)(6) The licensee shall ensure that all personnel authorized unescorted access to the protected area are trained and understand their roles and responsibilities during security incidents, to include hostage and duress situations.	This proposed requirement would be added to ensure that both security and non-security organization personnel are trained to recognize and respond to hostage and duress situations. This proposed training would also include the specific actions to be performed during these postulated security events.

§ 73.55(h)(4) Upon detection of abnormal presence or activity of persons or vehicles within an isolation zone, a protected area, material access area, or a vital area; or upon evidence or indication of intrusion into a protected area, a material access area, or a vital area, the licensee security organization shall:	(k)(7) Upon receipt of an alarm or other indication of threat, the licensee shall:	This requirement would be retained and revised for consistency with the proposed requirements of this section. Reference to the specific site areas would be deleted because the performance based requirements of this proposed section would be applicable to all facility areas, and therefore such reference would not be needed.
§ 73.55(h)(4)(i) Determine whether or not a threat exists,	(k)(7)(i) Determine the existence of a threat in accordance with assessment procedures.	This requirement would be retained with minor revision.
§ 73.55(h)(4)(ii) Assess the extent of the threat, if any,	(k)(7)(ii) Identify the level of threat present through the use of assessment methodologies and procedures.	This requirement would be retained with minor revision.
§ 73.55(h)(4)(iii)(A) Requiring responding guards or other armed response personnel to interpose themselves...	(k)(7)(iii) Determine the response necessary to intercept, challenge, delay, and neutralize the threat in accordance with the requirements of appendix C to part 73, the Commission-approved safeguards contingency plan, and the licensee response strategy.	This requirement would be retained with revision for consistency with the proposed paragraph (b) of this section.
§ 73.55(h)(4)(iii)(B) Informing local law enforcement agencies of the threat and requesting assistance.	(k)(7)(iv) Notify offsite support agencies such as local law enforcement, in accordance with site procedures.	This requirement would be retained with revision for consistency with the Integrated Response Plan.

§ 73.55(h)(2) The licensee shall establish and document liaison with local law enforcement authorities.	(k)(8) Law enforcement liaison. The licensee shall document and maintain current agreements with local, state, and Federal law enforcement agencies, to include estimated response times and capabilities.	This requirement would be retained with minor revision. Most significantly, this proposed requirement addresses the need to identify the resources and response times to be expected in order to facilitate planning development.
	(l) Facilities using mixed-oxide (MOX) fuel assemblies. In addition to the requirements described in this section for protection against radiological sabotage, operating commercial nuclear power reactors licensed under 10 CFR parts 50 or 52 and using special nuclear material in the form of MOX fuel assemblies shall protect unirradiated MOX fuel assemblies against theft or diversion.	This paragraph would be added to provide general provisions for the onsite physical protection of unirradiated mixed oxide (MOX) fuel assemblies in recognition of the fact that some nuclear power reactor facilities currently have chosen or may choose to possess and utilize this type of special nuclear material at their sites. Because weapons grade plutonium is utilized in the fabrication of MOX fuel assemblies, the Commission has determined that a threat of theft applies and that it is prudent and necessary to apply certain security measures for MOX fuel that are in addition to those that are currently required at other nuclear power reactor facilities. Therefore, the requirements proposed in this paragraph are provided to ensure that these additional requirements are identified and met by those licensees who have chosen or may choose to utilize MOX fuel.

	(l)(1) Licensees shall protect the unirradiated MOX fuel assemblies against theft or diversion in accordance with the requirements of this section and the approved security plans.	This requirement would be added to identify applicability of this paragraph.
	(l)(2) Commercial nuclear power reactors using MOX fuel assemblies are exempt from the requirements of §§ 73.20, 73.45, and 73.46 for the onsite physical protection of unirradiated MOX fuel assemblies.	This requirement would be added because the Commission has determined that due to the low plutonium concentration, composition of the MOX fuel, and configuration (size and weight) of the assemblies, the physical security protection measures identified in the listed regulations are superceded by those requirements addressed in this proposed section for unirradiated MOX fuel assemblies at nuclear power reactor facilities.
	(l)(3) Administrative controls.	This header would be added for formatting purposes.
	(l)(3)(i) The licensee shall describe in the approved security plans, the operational and administrative controls to be implemented for the receipt, inspection, movement, storage, and protection of unirradiated MOX fuel assemblies.	This requirement would be added to ensure that the licensee describes the onsite physical protection measures in the approved security plans.

	(l)(3)(ii) The licensee shall implement the use of tamper-indicating devices for unirradiated MOX fuel assembly transport and shall verify their use and integrity before receipt.	This requirement would be added to provide assurance that the unirradiated fuel assemblies were not accessed during transport.
	(l)(3)(iii) Upon delivery of unirradiated MOX fuel assemblies, the licensee shall:	This requirement would be added for formatting purposes.
	(l)(3)(iii)(A) Inspect unirradiated MOX fuel assemblies for damage.	This requirement would be added to ensure that unirradiated MOX fuel assemblies are in an acceptable condition before use or storage.
	(l)(3)(iii)(B) Search unirradiated MOX fuel assemblies for unauthorized materials.	This requirement would be added to ensure that no unauthorized materials were introduced within the unirradiated MOX fuel assembly during transport.
	(l)(3)(iv) The licensee may conduct the required inspection and search functions simultaneously.	This requirement would be added to provide a performance based requirement that provides flexibility for accomplishment of the proposed requirements.
	(l)(3)(v) The licensee shall ensure the proper placement and control of unirradiated MOX fuel assemblies as follows:	This requirement would be added for formatting purposes.

	(l)(3)(v)(A) At least one armed security officer, in addition to the armed response team required by paragraphs (h)(4) and (h)(5) of appendix C to part 73, shall be present during the receipt and inspection of unirradiated MOX fuel assemblies.	This requirement would be added to provide deterrence and immediate armed response to attempts of theft or tampering. This proposed armed responder's duty would be solely to observe and protect the unirradiated MOX fuel assemblies upon receipt and before storage.
	(l)(3)(v)(B) The licensee shall store unirradiated MOX fuel assemblies only within a spent fuel pool, located within a vital area, so that access to the unirradiated MOX fuel assemblies requires passage through at least three physical barriers.	This requirement would be added to reduce the risk of theft by providing three delay barriers before gaining unauthorized access to the MOX fuel assembles while in storage.
	(l)(3)(vi) The licensee shall implement a material control and accountability program for the unirradiated MOX fuel assemblies that includes a predetermined and documented storage location for each unirradiated MOX fuel assembly.	This requirement would be added to ensure that a material control and accountability program would be established and implemented and would focus on record keeping which describes the inventory and location of the SSNM within the assemblies.
	(l)(3)(vii) Records that identify the storage locations of unirradiated MOX fuel assemblies are considered safeguards information and must be protected and stored in accordance with § 73.21.	This requirement would be added to ensure restricted access to records which describe or identify the location of unirradiated MOX fuel assemblies within the spent fuel pool.
	(l)(4) Physical controls.	This header would be added for formatting purposes.

	(l)(4)(i) The licensee shall lock or disable all equipment and power supplies to equipment required for the movement and handling of unirradiated MOX fuel assemblies.	This requirement would be added to provide a performance based requirement for administrative controls over equipment and power supplies to equipment required to physically move the unirradiated MOX fuel assemblies to ensure that at least two security measures must be disabled before this equipment could be used.
	(l)(4)(ii) The licensee shall implement a two-person line-of-sight rule whenever control systems or equipment required for the movement or handling of unirradiated MOX fuel assemblies must be accessed.	This requirement would be added to provide an administrative control to reduce the risk of the insider threat and theft.
	(l)(4)(iii) The licensee shall conduct random patrols of areas containing unirradiated MOX fuel assemblies to ensure the integrity of barriers and locks, deter unauthorized activities, and to identify indications of tampering.	This requirement would be added to provide surveillance activities for the detection of unauthorized activities that would pose a threat to MOX fuel assemblies in addition to any similar requirements of this proposed section.
	(l)(4)(iv) Locks, keys, and any other access control device used to secure equipment and power sources required for the movement of unirradiated MOX fuel assemblies or openings to areas containing unirradiated MOX fuel assemblies must be controlled by the security organization.	This requirement would be added to ensure that the security organization would be responsible for the administrative controls over access control devices.

	(l)(4)(v) Removal of locks used to secure equipment and power sources required for the movement of unirradiated MOX fuel assemblies or openings to areas containing unirradiated MOX fuel assemblies must require approval by both the on-duty security shift supervisor and the operations shift manager.	This requirement would be added to ensure that both the licensee security and operations management level personnel would be responsible for the removal of locks securing MOX fuel assemblies.
	(l)(4)(v)(A) At least one armed security officer shall be present to observe activities involving the movement of unirradiated MOX fuel assemblies before the removal of the locks and providing power to equipment required for the movement or handling of unirradiated MOX fuel assemblies.	This requirement would be added to ensure that immediate armed response capability is provided before accessing equipment used to move unirradiated MOX fuel assemblies.
	(l)(4)(v)(B) At least one armed security officer shall be present at all times until power is removed from equipment and locks are secured.	This requirement would be added to ensure that immediate armed response capability is provided during any activity involving the use of equipment used to move unirradiated MOX fuel assemblies.
	(l)(4)(v)(C) Security officers shall be trained and knowledgeable of authorized and unauthorized activities involving unirradiated MOX fuel assemblies.	This requirement would be added to ensure that assigned security officers possess the capability to immediately recognize, report, and respond to unauthorized activities involving unirradiated MOX fuel assemblies.

	(l)(5) At least one armed security officer shall be present and shall maintain constant surveillance of unirradiated MOX fuel assemblies when the assemblies are not located in the spent fuel pool or reactor.	This requirement would be added to ensure physical protection of unirradiated MOX fuel assemblies when not located within an area that meets the three barrier requirement of this proposed rule.
	(l)(6) The licensee shall maintain at all times the capability to detect, assess, intercept, challenge, delay, and neutralize threats to unirradiated MOX fuel assemblies in accordance with the requirements of this section.	This requirement would be added for consistency with the proposed paragraph (b) of this section.
	(m) Digital computer and communication networks.	This header would be added for formatting purposes.
	(m)(1) The licensee shall implement a cyber-security program that provides high assurance that computer systems, which if compromised would likely adversely impact safety, security, and emergency preparedness, are protected from cyber attacks.	This requirement would be to ensure that nuclear power plants are protected from cyber attacks via minimizing the potential attack pathway and the consequences arising from a successful cyber attack.

	(m)(1)(i) The licensee shall describe the cyber-security program requirements in the approved security plans.	This requirement would be added to ensure licensees have a comprehensive security plan by integrating cyber-security into the overall onsite physical protection program. As licensees take advantage of computer technology to maximize plant productivity, the role of computer systems at nuclear power plants is increasing. Therefore, the Commission has determined that incorporation of a cyber-security program into the Commission-approved security plans would be a prudent and necessary security enhancement.
	(m)(1)(ii) The licensee shall incorporate the cyber-security program into the onsite physical protection program.	This requirement would be added to ensure that the computer systems used in onsite physical protection systems are protected from cyber attacks. With advancements in computer technology, many systems in nuclear power plants rely on computers to perform their functions, including some security functions. Therefore, the Commission has determined that the integration of security measures covering these systems would be a prudent and necessary action.

	(m)(1)(iii) The cyber-security program must be designed to detect and prevent cyber attacks on protected computer systems.	This requirement would be added to ensure licensees actively and pro-actively secure their plants from cyber attacks. The Commission has determined that because specific cyber threats and the people who seek unauthorized access to, or use of computers are constantly changing, protected computer systems must be protected against these attacks and mitigation measures implemented.
	(m)(2) Cyber-security assessment. The licensee shall implement a cyber-security assessment program to systematically assess and manage cyber risks.	This requirement would be added to require licensees to systematically determine the status of their plant's cyber risks and identify vulnerabilities that need to be mitigated to reduce risks to acceptable levels.
	(m)(3) Policies, requirements, and procedures.	This header would be added for formatting purposes.
	(m)(3)(i) The licensee shall apply cyber-security requirements and policies that identify management expectations and requirements for the protection of computer systems.	This requirement would be added to create a computer security program that establishes specific goals and assigns responsibilities to employees to meet those goals.
	(m)(3)(ii) The licensee shall develop and maintain implementing procedures to ensure cyber-security requirements and policies are implemented effectively.	This requirement would be added to ensure the licensee develops, implements, and enforces, detailed guidance documents that licensee employees would be required to follow to meet the stated security goals.

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

	(m)(4)(ii) The cyber-security incident response and recovery plan must be described in the integrated response plan required by appendix C to this part.	This requirement would be added to ensure licensees have a comprehensive incident response plan by integrating cyber-security into the overall security of their plants. As licensees take advantage of computer technology to maximize plant productivity, the role of computer systems at nuclear power plants is increasing as well as the possibility for adverse impact from a computer mishap. Therefore, the Commission has determined that it would be a prudent and necessary action for licensees to develop and implement a comprehensive response plan that includes a cyber incident response and recovery plan.
	(m)(4)(iii) The cyber-security incident response and recovery plan must ensure the capability to respond to cyber-security incidents, minimize loss and destruction, mitigate and correct the weaknesses that were exploited, and restore systems and/or equipment affected by a cyber-security incident.	This requirement would be added to ensure that licensees acquire the capability to respond to cyber incidents in a manner that contains and repairs damage from incidents, and prevents future damage. An incident handling capability provides a way for plant personnel to report incidents and the appropriate response and assistance to be provided to aid in recovery.

	(m)(5) Protective strategies. The licensee shall implement defense-in-depth protective strategies to protect computer systems from cyber attacks, detecting, isolating, and neutralizing unauthorized activities in a timely manner.	This requirement would be added to incorporate the approach of delay, detect, and respond. The use of multiple and diverse layers of defense would delay the threat from reaching those systems that, if compromised, can adversely impact safety, security, or emergency preparedness of the nuclear power plants. This delay in attack would allow more time to detect the attack and would allow time to respond.
	(m)(6) Configuration and control management program. The licensee shall implement a configuration and control management program, to include cyber risk analysis, to ensure that modifications to computer system designs, access control measures, configuration, operational integrity, and management process do not adversely impact facility safety, security, and emergency preparedness systems before implementation of those modifications.	This requirement would be added to implement configuration management to ensure that the system in operation is the correct version (configuration) of the system and that any changes to be made are reviewed for security implications. Configuration management can be used to help ensure that changes take place in an identifiable and controlled environment and that they do not unintentionally harm any of the system's properties, including its security.
	(m)(7) Cyber-security awareness and training.	This header would be added for formatting purposes.

	(m)(7)(i) The licensee shall implement a cyber-security awareness and training program.	This requirement would be added to ensure licensees implement cyber-security awareness and training programs to ensure that appropriate personnel are aware of cyber-security requirements and have the cyber-security skills and competencies necessary to secure affected plant systems and equipment.
	(m)(7)(ii) The cyber-security awareness and training program must ensure that appropriate plant personnel, including contractors, are aware of cyber-security requirements and that they receive the training required to effectively perform their assigned duties and responsibilities.	This requirement would be added to implement a cyber-security awareness and training program to: 1. Improve employee awareness of the need to protect computer systems; 2. Develop employee skills and knowledge so computer users can perform their jobs more securely; and 3. Build in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.
	(n) Security program reviews and audits.	This header would be added for formatting purposes.
§ 73.55(g)(4)(i)(A) At intervals not to exceed 12 months or...	(n)(1) The licensee shall review the onsite physical protection program at intervals not to exceed 12 months, or	This requirement would be retained with minor revision for formatting purposes.
§ 73.55(g)(4)(i)(B) As necessary, based on an assessment by the licensee against performance indicators ...	(n)(1)(i) As necessary based upon assessments or other performance indicators.	This requirement would be retained with minor revision.

§ 73.55(g)(4)(i)(B) ...as soon as reasonably practicable after a change occurs in personnel, procedures, equipment, or facilities that potentially could adversely affect security but no longer than 12 months after the change.	(n)(1)(ii) Within 12 months after a change occurs in personnel, procedures, equipment, or facilities that potentially could adversely affect security.	This requirement would be retained and revised. Most significantly, the phrase "as soon as reasonably practicable" would be deleted and the current requirement "12 months" would be moved to the beginning of the sentence to eliminate potential for misunderstanding and improve consistency.
§ 73.55(g)(4)(i)(B) In any case, each element of the security program must be reviewed at least every 24 months.	(n)(2) As a minimum, each element of the onsite physical protection program must be reviewed at least every twenty-four (24) months.	This requirement would be retained with minor revision.
§ 73.55(g)(4)(i) The licensee shall review implementation of the security program by individuals who have no direct responsibility for the security program either: § 73.55(g)(4)(ii) The results and recommendations of the security program review... must be documented...	(n)(2)(i) The onsite physical protection program review must be documented and performed by individuals independent of those personnel responsible for program management and any individual who has direct responsibility for implementing the onsite physical protection program.	This requirement would be retained and revised to combine two current requirements. Most significantly, the word "documented" would be added for consistency with the current § 73.55(g)(4)(ii). The phrase "security program" would be replaced with the phrase "program" for consistency with use of the phrase "onsite physical protection program".

§ 73.55(g)(4)(ii) The security program review must include an audit of security procedures and practices, an evaluation of the effectiveness of the physical protection system, an audit of the physical protection system testing and maintenance program, and an audit of commitments established for response by local law enforcement authorities.	(n)(2)(ii) Onsite physical protection program reviews and audits must include, but not be limited to, an evaluation of the effectiveness of the approved security plans, implementing procedures, response commitments by local, state, and Federal law enforcement authorities, cyber-security programs, safety/security interface, and the testing, maintenance, and calibration program.	This requirement would be retained and revised to provide additional examples. Most significantly, the phrase "but not be limited to" would be added to clarify that the proposed examples are not all inclusive.
§ 73.55(d)(7)(ii)(B) Periodically review physical security plans and contingency plans and procedures to evaluate their potential impact on plant and personnel safety.	(n)(3) The licensee shall periodically review the approved security plans, the integrated response plan, the licensee protective strategy, and licensee implementing procedures to evaluate their effectiveness and potential impact on plant and personnel safety.	This requirement would be retained with minor revision. The phrase “Integrated Response Plan” would be added to emphasize the importance of this proposed plan and to emphasize its relationship to other site plans. The term ”implementing” procedures would be added for consistency with this proposed section.
	(n)(4) The licensee shall periodically evaluate the cyber-security program for effectiveness and shall update the cyber-security program as needed to ensure protection against changes to internal and external threats.	This requirement would be added to account for the use of computers and the need to ensure that required protective measures are being met and to evaluate the effects that changes or other technological advancements would have on systems used at nuclear power plants.

	(n)(5) The licensee shall conduct quarterly drills and annual force-on-force exercises in accordance with appendix C to part 73 and the licensee performance evaluation program.	This requirement would be added to provide a performance based requirement for the conduct force-on-force drills and exercises.
§ 73.55(g)(4)(ii) The results and recommendations of the security program review, management's findings on whether the security program is currently effective, 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 the day-to-day plant operation.	(n)(6) The results and recommendations of the onsite physical protection program reviews and audits, management's findings regarding program effectiveness, and any actions taken as a result of recommendations from prior program reviews, must be documented in a report to the licensee's plant manager and to corporate management at least one level higher than that having responsibility for day-to-day plant operation.	This requirement would be retained with minor revision. The phrase "security program review" would be replaced with the phrase" onsite physical protection program reviews and audits" for consistency with the format of the proposed rule. The phrase "on whether the security program is currently effective" would be replaced with the phrase "regarding program effectiveness” for plain language purposes.
	(n)(7) Findings from onsite physical protection program reviews, audits, and assessments must be entered into the site corrective action program and protected as safeguards information, if applicable.	This requirement would be added to ensure that security deficiencies and findings would be tracked through the site corrective action program until corrected, and information regarding specific findings would be protected in accordance with the sensitivity and potential for exploitation of the information.

	(n)(8) The licensee shall make changes to the approved security plans and implementing procedures as a result of findings from security program reviews, audits, and assessments, where necessary to ensure the effective implementation of Commission regulations and the licensee protective strategy.	This requirement would be added to provide a performance based requirement for the revision of approved security plans where plan changes are necessary to account for implementation problems, changes to site conditions, or other problems that adversely affect the licensee capability to effectively implement Commission requirements.
	(n)(9) Unless otherwise specified by the Commission, onsite physical protection program reviews, audits, and assessments may be conducted up to thirty days prior to, but no later than thirty days after the scheduled date without adverse impact upon the next scheduled annual audit date.	This requirement would be added to provide necessary flexibility to allow licensees to conduct audits/reviews within a specified time period without changing future scheduled audit/review dates. This requirement provides regulatory stability and flexibility to account for unforseen circumstances that may interfere with regularly scheduled dates, such as forced outages.
§ 73.55(g) Testing and maintenance.	(o) Maintenance, testing, and calibration.	This header would be retained and revised to include "calibration" of equipment to ensure the accuracy of readings provided from such equipment.
	(o)(1) The licensee shall:	This header would be added for formatting purposes.

	(o)(1)(i) Implement a maintenance, testing and calibration program to ensure that security systems and equipment are tested for operability and performance at predetermined intervals, are maintained in operable condition, and are capable of performing their intended function when needed.	This requirement would be added to comprehensively address all security equipment in consistent terms. This proposed requirement would clarify the current requirement for ensuring that security equipment operates and performs as stated in the approved security plans.
	(o)(1)(ii) Describe the maintenance, testing and calibration program in the approved physical security plan. Implementing procedures must specify operational and technical details required to perform maintenance, testing, and calibration activities to include, but not limited to, purpose of activity, actions to be taken, acceptance criteria, the intervals or frequency at which the activity will be performed, and compensatory actions required.	This requirement would be added to address the maintenance, testing and calibration of security equipment in non-specific terms and describe the types of documentation and level of detail needed.
	(o)(1)(iii) Document problems, failures, deficiencies, and other findings, to include the cause of each, and enter each into the site corrective action program. The licensee shall protect this information as safeguards information, if applicable.	This requirement would be added for consistency with the proposed requirement for addressing findings from security program reviews and audits and how specific information concerning security deficiencies and findings must be protected so that noted deficiencies could not be exploited.

§ 73.55(g)(1) The licensee shall develop and employ compensatory measures including equipment, additional security personnel and specific procedures to assure that the effectiveness of the security system is not reduced by failure or other contingencies affecting the operation of the security related equipment or structures.	(o)(1)(iv) Implement compensatory measures in a timely manner to ensure that the effectiveness of the onsite physical protection program is not reduced by failure or degraded operation of security-related components or equipment.	This requirement would be retained with minor revision.
§ 73.55(g)(2) Each intrusion alarm shall be tested for performance at the beginning and end of any period that it is used for security. If the period of continuous use is longer than seven days, the intrusion alarm shall also be tested at least once every seven (7) days.	(o)(2) Each intrusion alarm must be tested for operability at the beginning and end of any period that it is used for security, or if the period of continuous use exceeds seven (7) days, the intrusion alarm must be tested at least once every seven (7) days.	This requirement would be retained and revised to correct the use of the phrase "tested for performance", as stated in the current § 73.55(g)(2). The testing performed at the beginning and end of any period is intended to be a "go, no-go" test or operational test that is used to simply indicate that the equipment functions in response to predetermined stimuli. A performance test is a more elaborate test that would test a system through the entire range of its intended function or stimuli.

§ 73.55(g)(2) Each intrusion alarm shall be tested for performance at the beginning and end of any period that it is used for security.	(o)(3) Intrusion detection and access control equipment must be performance tested in accordance with the approved security plans.	This requirement would be retained and revised to correct the periodicity of performance testing stated in the current § 73.55(g)(2) and to add "access control equipment" due to the widespread use of access control technologies and to focus on the need to ensure that this equipment is functioning as intended in response to the predetermined stimuli (e.g., biometrics). The phrase "each intrusion alarm" would be replaced with the phrase "Intrusion detection and access control equipment" to more accurately describe the equipment to be performance tested.
§ 73.55(g)(3) Communications equipment required for communications onsite shall be tested for performance not less frequently than once at the beginning of each security personnel work shift.	(o)(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.	This proposed requirement would be retained and revised to correct the use of the phrase "tested for performance", as stated in the current § 73.55 (g)(3). The testing performed at the beginning and end of any period is intended to be a "go, no-go" test or operational test that is used to simply indicate that the equipment functions in response to predetermined stimuli.

§ 73.55(g)(3) Communications equipment required for communications offsite shall be tested for performance not less than once a day.	(o)(5) Communication systems between the alarm stations and each control room, and between the alarm stations and offsite support agencies, to include back-up communication equipment, must be tested for operability at least once each day.	This requirement would be retained and revised to include both "onsite" and offsite communication equipment associated with integrated response and to correct the use of the term “performance test,” as stated in the current § 73.55 (g)(3). The testing performed at least once each day is intended to be a "go, no-go" test or operational test that is used to simply indicate that the equipment functions.
	(o)(6) Search equipment must be tested for operability at least once each day and tested for performance at least once during each seven (7) day period and before being placed back in service after each repair or inoperative state.	This requirement would be added to ensure that search equipment is tested for operability and performance at intervals that provide assurance that unauthorized items would be detected as required. This proposed requirement is added to address the widespread use of search equipment technologies, such as explosives and metal detectors, and x-ray equipment and to provide a performance based requirement that focuses on the importance for accurate performance of this equipment.
§ 73.55(g)(1) All alarms, communication equipment, physical barriers, and other security related devices or equipment shall be maintained in operable condition.	(o)(7) All intrusion detection equipment, communication equipment, physical barriers, and other security-related devices or equipment, to include back-up power supplies must be maintained in operable condition.	This requirement would be retained with minor revision. Most significantly, back-up power supplies are added to ensure this critical element is maintained in operable condition.

	(o)(8) A program for testing or verifying the operability of devices or equipment located in hazardous areas must be specified in the approved security plans and must define alternate measures to be taken to ensure the timely completion of testing or maintenance when the hazardous condition or radiation restrictions are no longer applicable.	This requirement would be added to account for those circumstances when a licensee can not satisfy testing requirements due to safety hazards or radiation restrictions. Vital component area portals located within facility radiological controlled areas that are inaccessible due to safety hazards or established radiation restrictions may be excluded from the testing requirements of this section.
	(p) Compensatory measures.	This header would be added for formatting purposes.
§ 73.55(g)(1) The licensee shall develop and employ compensatory measures...	(p)(1) The licensee shall identify measures and criteria needed to compensate for the loss or reduced performance of personnel, equipment, systems, and components, that are required to meet the requirements of this section.	This requirement would be retained with minor revision. The word "compensate" is used to provide a performance based requirement that requires the identified compensatory measure to be "developed and employed".
§ 73.55(g)(1) The licensee shall develop and employ compensatory measures including equipment, additional security personnel and specific procedures to assure that the effectiveness of the security system is not reduced by failure or other contingencies affecting the operation of the security related equipment or structures.	(p)(2) Compensatory measures must be designed and implemented to provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable personnel, equipment, system, or components.	This requirement would be retained and revised to focus on the Commission's view that compensatory measures must provide a level of protection that satisfies the Commission requirement which was otherwise satisfied through use or implementation of the failed component of the onsite physical protection program.

	(p)(3) Compensatory measures must be implemented within specific time lines necessary to meet the requirements stated in paragraph (b) of this section and described in the approved security plans.	This requirement would be added to provide a performance based requirement for timely implementation of compensatory measures. The phrase "within specific time lines necessary to meet the requirements stated in paragraph (b)" would provide qualifying details against which specific time lines would be developed.
	(q) Suspension of safeguards measures.	This header would be added for formatting purposes.
	(q)(1) The licensee may suspend implementation of affected requirements of this section under the following conditions:	This requirement would be added for formatting purposes. The phrase "implementation of affected requirements" would be used to ensure the licensee only suspends those measures that cannot be met as a direct result of the condition.
§ 73.55(a) In accordance with §§ 50.54(x) and 50.54(y) of this chapter, the licensee may suspend any safeguards measures pursuant to § 73.55 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 specification that can provide adequate or equivalent protection is immediately apparent.	(q)(1)(i) In accordance with §§ 50.54(x) and 50.54(y) of this chapter, the licensee may suspend any safeguards measures pursuant to this section in an emergency when this action is immediately needed to protect the public health and safety and no action consistent with license conditions and technical specifications that can provide adequate or equivalent protection is immediately apparent.	This requirement would be retained with minor revision.

§ 73.55(a) This suspension must be approved as a minimum by a licensed senior operator prior to taking the action.	This suspension of safeguards measures must be approved as a minimum by a licensed senior operator prior to taking this action.	This requirement would be retained with minor revision to report this information to the control room. This proposed requirement is intended to ensure that at least one onsite, licensee management level person who is knowledgeable and aware of reactor operations and reactor status at the time, is the individual who would approve the suspension and has the knowledge to determine and the authority to direct appropriate compensatory measures to include, but not limited to, modifications to the licensee protective strategy during the suspension period.
	(q)(1)(ii) During severe weather when the suspension is immediately needed to protect personnel whose assigned duties and responsibilities in meeting the requirements of this section would otherwise constitute a life threatening situation and no action consistent with the requirements of this section that can provide equivalent protection is immediately apparent. Suspension of safeguards due to severe weather must be initiated by the security supervisor and approved by a licensed senior operator prior to taking this action.	This requirement would be added to provide a performance based requirement that accounts for the suspension of safeguards measures during severe weather conditions that could result in life threatening situations such as tornadoes, floods, hurricanes, etc., for those individuals assigned to carry out certain duties and responsibilities required by Commission regulations, and the approved security plans and procedures. This requirement would be added to provide a requirement for who is authorized to approve suspensions under severe weather conditions.

	(q)(2) Suspended security measures must be reimplemented as soon as conditions permit.	This requirement would be added to provide a performance based requirement for reimplementing suspended security measures.
§ 73.55(a) The suspension of safeguards measures must be reported in accordance with the provisions of § 73.71.	(q)(3) The suspension of safeguards measures must be reported and documented in accordance with the provisions of § 73.71.	This requirement would be retained with minor revision for documenting suspended security measures.
§ 73.55(a) Reports made under Section § 50.72 need not be duplicated under § 73.71.	(q)(4) Reports made under § 50.72 of this chapter need not be duplicated under § 73.71.	This requirement would be retained.
	(r) Records.	This header would be added for formatting purposes.
§ 73.55(b)(1)(ii) The NRC may inspect, copy, and take away copies of all reports and documents required to be kept by Commission regulations, orders, or applicable license conditions whether the reports and documents are kept by the licensee or the contractor,	(r)(1) The Commission may inspect, copy, retain, and remove copies of all records required to be kept by Commission regulations, orders, or license conditions whether the records are kept by the licensee or a contractor.	This requirement would be retained with minor revision. The phrase "reports and documents" would be replaced with the word "records" to account for all information collection requirements regardless of media, to include electronic record keeping systems.

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

§ 73.55(a) The Commission may authorize an applicant or licensee to provide measures for protection against radiological sabotage other than those required by this section if the applicant or licensee demonstrates that the measures have the same high assurance objective as specified in this paragraph and that the overall level of system performance provides protection against radiological sabotage equivalent to that which would be provided by Paragraphs (b) through (h) of this section and meets the general performance requirements of this section.	(t)(1) The Commission may authorize an applicant or licensee to provide a measure for protection against radiological sabotage other than one required by this section if the applicant or licensee demonstrates that: (i) The measure meets the same performance objective and requirements as specified in paragraph (b) of this section, and (ii) The proposed alternative measure provides protection against radiological sabotage or theft of unirradiated MOX fuel assemblies, equivalent to that which would be provided by the specific requirement for which it would substitute.	This requirement would be retained and revised to provide a performance based requirement for alternative measures that focus attention on the Commission's view that an alternative measure is an unanalyzed substitute for a specific Commission requirement of this proposed section and therefore, must be individually and knowingly reviewed and approved by the Commission before implementation to ensure consistency with these proposed Commission regulations. The Commission has determined that the requirements described in this proposed section have been carefully analyzed by the Commission and therefore, an alternative measure to a proposed requirement of this section must also be carefully analyzed through the process addressed in 10 CFR 50.90 before implementation. Specifically, the language used by this proposed requirement addresses alternative measures "individually" rather than collectively to clarify that each proposed alternative measure is unique by itself and must be analyzed as such. In addition, the phrase "have the same high assurance objective" is replaced with the phrase "meets the same performance objective and requirements as specified in paragraph (b) of this section".

		The proposed paragraph (b) of this section retains the same "high assurance objective" referred to by the current requirement and incorporates by reference the performance based requirements of this proposed section that facilitate licensee achievement of the intended high assurance objective.
§ 73.55(c)(9)(i) For licensees who choose to propose alternative measures as provided for in 10 CFR 73.55 (c)(8), the proposal must be submitted in accordance with 10 CFR 50.90 and include the analysis and justification for the proposed alternatives.	(t)(2) The licensee shall submit each proposed alternative measure to the Commission for review and approval in accordance with §§ 50.4 and 50.90 of this chapter before implementation.	This requirement would be retained and revised to expand the application of the current provision for alternative measures to all proposed requirements of this section and would provide the process by which alternative measures would be submitted for Commission review and approval.
§ 73.55(c)(8)(ii) Propose alternative measures, in addition to the measures established in accordance with 10 CFR 73.55 (c)(7), describe the level of protection that these measures would provide against a land vehicle bomb, and compare the costs of the alternative measures with the costs of measures necessary to fully meet the design goals and criteria.	(t)(3) The licensee shall submit a technical basis for each proposed alternative measure, to include any analysis or assessment conducted in support of a determination that the proposed alternative measure provides a level of protection that is at least equal to that which would otherwise be provided by the specific requirement of this section.	This requirement would be retained and revised to expand the application of the current provision for alternative measures to all proposed requirements of this section and to provide a description of the detailed information needed to support the technical basis for a request for Commission approval of an alternative measure.

§ 73.55(c)(8)(ii) The Commission will approve the proposed alternative measures if they provide substantial protection against a land vehicle bomb, and it is determined by an analysis, using the essential elements of 10 CFR 50.109, that the costs of fully meeting the design goals and criteria are not justified by the added protection that would be provided.	(t)(4) Alternative vehicle barrier systems. In the case of alternative vehicle barrier systems required by § 73.55(e)(8), the licensee shall demonstrate that: (i) The alternative measure provides substantial protection against a vehicle bomb, and (ii) Based on comparison of the costs of the alternative measures to the costs of meeting the Commission's requirements using the essential elements of 10 CFR 50.109, the costs of fully meeting the Commission's requirements are not justified by the protection that would be provided.	This requirement would be retained with minor revision. The phrase "The Commission will approve the proposed alternative measures" would be deleted because approval would be based on NRC review. The proposed language clearly stipulates that alternative measures will be reviewed by the staff and approval would be contingent upon the justification provided by the licensee to include an analysis that examines the costs and benefits of the alternative measure consistent with 10 CFR 50.109.
	73.55 Definitions.	This requirement would be added to clarify the use of the listed terms used in this proposed rule.
	Security Officer means a uniformed individual, either armed with a covered weapon or unarmed, whose primary duty is the protection of a facility, of radioactive material, or of other property against theft or diversion or against radiological sabotage.	This definition would be added to clarify what is meant by the term "Security Officer" as used in this document.

	Target Set means 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 (e.g., non-incipient, non-localized fuel melting, and/or core disruption) barring extraordinary action by plant operators. A target set with respect to spent fuel sabotage is draining the spent fuel pool leaving the spent fuel uncovered for a period of time, allowing spent fuel heat-up and the associated potential for release of fission products.	This definition would be added to clarify what is meant by the term Target Set" as used in this document.

Table 3 - Proposed Part 73 Section 73.56
Personnel access authorization requirements for nuclear power plants.

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
§ 73.56(a) General	(a) Introduction.	This header would be added for formatting purposes. This proposed § 73.56(a) would amend and reorganize current § 73.56(a) [General]. The current §73.56(a) required licensees to develop and implement access authorization (AA) programs. The proposed § 73.56(a) would update these requirements. The title of this paragraph would be revised to more accurately capture the topics addressed in the proposed § 73.56(a), which would include a description of the NRC-regulated entities who would be subject to the section and the methods by which the NRC intends that licensees would implement the amended AA programs. These proposed changes to the language and organization of current § 73.56(a) would be made to enhance the clarity of the requirements in this section, for the reasons discussed in Section IV.

§ 73.56(a) *General.* (1) Each licensee who is authorized on April 25, 1991, to operate a nuclear power reactor pursuant to §§50.21(b) or 50.22 of this chapter shall comply with the requirements of this section. By April 27, 1992, the required access authorization program must be incorporated into the site Physical Security Plan as provided for by 10 CFR 50.54(p)(2) and implemented. By April 27, 1992, each licensee shall certify to the NRC that it has implemented an access authorization program that meets the requirements of this part.	(a)(1) By [date - 180 days - after the effective date of the final rule published in the Federal Register], each nuclear power reactor licensee, licensed under 10 CFR part 50, shall incorporate the revised requirements of this section through amendments to its Commission-approved access authorization program and shall submit the amended program to the Commission for review and approval.	This requirement would be added to discuss the types of Commission licensees to whom the proposed requirements of this section would apply and the schedule for submitting the amended access authorization program. The Commission intends to delete the current language, because it applies only to a past rule change that is completed. The proposed requirements of this section would be applicable to decomissioned/ing reactors unless otherwise approved by the Commission. This proposed requirement would add a requirement for Commission review and approval of the amended access authorization program to ensure that access authorization programs meet the objective of providing high assurance that individuals who are subject to the requirements of this section are trustworthy and reliable, and do not constitute an unreasonable risk to public health and safety or the common defense and security, including the potential to commit radiological sabotage.
	(a)(2) The amended program must be submitted as specified in § 50.4 and must describe how the revised requirements of this section will be implemented by the licensee, to include a proposed implementation schedule.	This requirement would be added to provide a reference to the current § 50.4(b)(4) which describes procedural details relative to the proposed security plan submission requirement.

	(a)(3) The licensee shall implement the existing approved access authorization program and associated Commission orders until Commission approval of the amended program, unless otherwise authorized by the Commission.	This requirement would be added to clarify that the licensee must continue to implement the current Commission-approved security plans until the Commission approves the amended plans. The phrase “unless otherwise authorized by the Commission” would provide flexibility to account for unanticipated situations that may affect the licensee's ability to comply with this proposed requirement.
	(a)(4) The licensee is responsible to the Commission for maintaining the authorization program in accordance with Commission regulations and related Commission-directed orders through the implementation of the approved program and site implementing procedures.	This requirement would be added to clarify that the licensee is responsible for meeting Commission regulations and the approved security plans. The phrase “through the implementation of the approved program and site implementing procedures” would be added to describe the relationship between Commission regulations, the approved authorization program, and implementing procedures. The Commission views the approved security plans as the mechanism through which the licensee implements Commission requirements.

§ 73.56(a)(2) Each applicant for a license to operate a nuclear power reactor pursuant to §§ 50.21(b) or 50.22 of this chapter, whose application was submitted prior to April 25, 1991, shall either by April 27, 1992, or the date of receipt of the operating license, whichever is later, incorporate the required access authorization program into the site Physical Security Plan and implement it. § 73.56(a)(3) Each applicant for a license to operate a nuclear power reactor pursuant to §§ 50.21(b) or 50.22 of this chapter and each applicant for a combined construction permit and operating license pursuant to part 52 of this chapter, whose application is submitted after April 25, 1991, shall include the required access authorization program as part of its Physical Security Plan. The applicant, upon receipt of an operating license or upon receipt of operating authorization, shall implement the required access authorization program as part of its site Physical Security Plan.	(a)(5) Applicants for an operating license under the provisions of part 50 of this chapter, or holders of a combined license under the provisions of part 52 of this chapter, shall satisfy the requirements of this section upon receipt of an operating license or upon notice of the Commission's finding under § 52.103(g) of this chapter.	This requirement would be added to describe the proposed requirements for applicants and to specify that the proposed requirements of this section must be met upon receipt of an operating license or upon notice of the Commission's finding under § 52.103(g) of this chapter. This proposed requirement would retain the meaning of the current § 73.56(a)(3), which requires applicants for a license to operate a nuclear power plant to incorporate an access authorization program in their Physical Security Plan and implement the approved access authorization program when approval to begin operating is received. This proposed requirement would also add a requirement for Commission review and approval of an applicant's Physical Security Plan incorporating the requirements of this proposed section for the reasons discussed with respect to proposed § 73.56(a)(1). The Commission intends to delete the current § 73.56(a)(2) because there are no remaining applicants for an operating license under §§ 50.21(b) or 50.22 of this chapter who have not implemented an AA program under the current requirements. Therefore, the current paragraph is no longer necessary.

		The proposed paragraph would retain the current requirement for licensees and applicants to implement access authorization programs upon receipt of an operating license or operating authorization, respectively, and add a requirement for these entities to maintain their access authorization programs. The requirement to maintain AA programs would be added to convey more accurately that § 73.56 includes requirements for maintaining AA programs, in addition to requirements for implementing them.
§ 73.56(a)(4) The licensee may accept part of an access authorization program used by its contractors, vendors, or other affected organizations and substitute, supplement, or duplicate any portion of the program as necessary to meet the requirements of this section. In any case, the licensee is responsible for granting, denying, or revoking unescorted access authorization to any contractor, vendor, or other affected organization employee.	(a)(6) Contractors and vendors (C/Vs) who implement authorization programs or program elements shall develop, implement, and maintain authorization programs or program elements that meet the requirements of this section, to the extent that the licensees and applicants specified in paragraphs (a)(1) and (a)(5) of this section rely upon those C/V authorization programs or program elements to meet the requirements of this section. In any case, only a licensee or applicant shall grant or permit an individual to maintain unescorted access to nuclear power plant protected and vital areas.	Proposed § 73.56(a)(6) would amend current § 73.56(a)(4), which permits licensees to accept a C/V authorization program to meet the standards of this section. The proposed paragraph would retain the current permission for licensees to accept C/V authorization programs, in full or in part, but would also add C/Vs to the list of entities who are subject to proposed § 73.56 in order to convey more clearly that C/Vs may be directly subject to NRC inspection and enforcement actions than the current rule language implies.

		This change is necessary to clarify the applicability of the rule's requirements to a C/V's authorization program because several requirements in the current section could be interpreted as implying that a C/V is accountable to the licensee but not to the NRC, should significant weaknesses be identified in the C/V's authorization program upon which one or more licensees rely. However, this interpretation would be incorrect. Therefore, proposed § 73.56(a)(6) would include C/V authorization programs and program elements upon which licensees and applicants rely within the scope of this section to convey more accurately that these C/Vs are directly accountable to the NRC for meeting the applicable requirements of § 73.56. This clarification is also necessary to maintain the internal consistency of the proposed rule because some provisions of the proposed section apply only to C/Vs, including, but not limited to, the second sentence of proposed § 73.56(n)(7). The proposed paragraph would also retain the intent of the current requirement that only licensees and applicants have the authority to grant or permit an individual to maintain unescorted access to nuclear power plant protected and vital areas.

		The phrases, “program elements” and “to the extent that...,” would replace the second sentence of current § 73.56(a)4), which permits licensees to accept part of an authorization program used by its contractors, vendors, or other affected organizations and substitute, supplement, or duplicate any portion of the program as necessary to meet the requirements of this section. The proposed change would retain the meaning of the current provision, but would clarify the intent of the provision in response to implementation questions from licensees. The phrase, “program elements,” would replace “part of an access authorization program,” to more clearly convey that the parts of an authorization program to which this provision refers are the program elements that are required under current and proposed § 73.56, including a background investigation; psychological assessment; behavioral observation; a review procedure for adverse determinations regarding an individual’s trustworthiness and reliability; audits; the protection of information; and retaining and sharing records.

		The phrase, “to the extent that the licensees and applicants rely upon C/V authorization programs or program elements,” would be used in proposed § 73.56(a)(6) to clarify that C/Vs need only meet the requirements of this section for those authorization program elements upon which licensees and applicants who are subject to this section rely. This change would be made to address two issues. First, “to the extent that” would be used to indicate that C/Vs need not implement every element of an AA program in order for licensees to rely on the program elements that a C/V does implement in accordance with the requirements of this section. For example, if a C/V conducts background investigations upon which licensees rely in making unescorted access authorization determinations, the background investigations must meet the requirements of current § 73.56(b)(2)(i) [or proposed § 73.56(d)]. However, the C/V need not also perform psychological assessments or any other services for licensees in order for licensees to rely on the background investigations that the C/V performs. Second, the phrase, “to the extent that,” would also indicate that any elements of an authorization program that a C/V implements that are not relied upon by licensees need not meet the requirements of this section.

		For example, if the same C/V in the previous example also offers psychological assessment services, in addition to conducting background investigations for licensees, but no licensees or applicants who are subject to this section rely on those psychological assessment services to make unescorted access authorization decisions, then the C/V need not meet the requirements of current § 73.56(b)(2)(ii) [or proposed § 73.56(e)] for conducting those psychological assessments. These proposed changes to the terms used in current § 73.56(a)(4) would be made for increased clarity in the language of the rule.
	(b) Individuals who are subject to an authorization program. (b)(1) The following individuals shall be subject to an authorization program:	A new § 73.56(b) [Individuals who are subject to an AA program] would specify the individuals who must be subject to an AA program, based on their job duties and responsibilities. Current § 73.56 requires only that individuals who have unescorted access to protected and vital areas shall be subject to an AA program. The proposed rule would add several categories of individuals who would be subject to the proposed AA program, for the reasons discussed with respect to each paragraph that addresses the additional categories of individuals who would be covered.

		Proposed § 73.56(b) would be added for clarity in the organization of the proposed section by grouping together in one list the individuals who would be subject to the proposed regulations.
§ 73.56(b) *General performance objective and requirements.* (1) The licensee shall establish and maintain an access authorization program granting individuals unescorted access to protected and vital areas....	(b)(1)(i) Any individual to whom a licensee or applicant grants unescorted access to nuclear power plant protected and vital areas.	Proposed § 73.56(b)(1)(i) would retain the current requirement that any individual who has unescorted access to nuclear power plant protected and vital areas shall be subject to an AA program that meets the requirements of this section. The current requirement is embedded in the first sentence of current § 73.56(b) [General performance objective and requirements]. The proposed paragraph would list this category of individuals separately for organizational clarity in the rule.
	(b)(1)(ii) Any individual whose assigned duties and responsibilities permit the individual to take actions by electronic means, either onsite or remotely, that could adversely impact a licensee's or applicant's operational safety, security, or emergency response capabilities; and	A new § 73.56(b)(1)(ii) would require that individuals who are assigned duties and responsibilities that permit them to take actions by electronic means that could adversely impact a licensee's or applicant's operational safety, security, or emergency response capabilities would be subject to an AA program.

		The proposed provision would be consistent with the intent of current § 73.56, which is to ensure that anyone who has unescorted access to equipment that is important to the operational safety and security of plant operations must be trustworthy and reliable. As discussed in Section IV.3, because of the increased use of digital systems and advanced communications technologies in nuclear power plants, the current regulations, which focus on individuals who have physical access to equipment within protected and vital areas, do not provide adequate assurance of the trustworthiness and reliability of persons whose job duties and responsibilities permit them to take actions through electronic means that can affect operational safety, security, and emergency response capabilities, but who, because of advances in electronic communications, may not require physical access to protected and vital areas. For example, some licensees have installed systems that permit engineers or information technology technicians to take actions from remote locations that may affect the operability of safety-related components, or affect the functionality of operating systems.

		Because the potential impact of actions taken through electronic means may be as serious as actions taken by an individual who is physically present within a protected or vital area, the NRC has determined that subjecting this additional category of individuals to the AA program is necessary.
	(b)(1)(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	Proposed § 73.56(b)(1)(iii) would require that certain individuals who are members of the licensee's or applicant's security organization shall be subject to an AA program, based on their responsibilities for implementing a licensee's protective strategy. Current § 73.55 requires that any armed members of the security organization must be subject to an AA program, but the proposed rule would also list them here for clarity and completeness in the requirements of this section. The proposed paragraph would also include any individual who has responsibilities for implementing the licensee's protective strategy, which may include individuals who are not armed. In practice, the NRC is not aware of any licensees, applicants, or C/Vs who do not subject this broader category of individuals to an AA program.

		However, the proposed rule would specify that these individuals shall be subject to an AA program because of their critical responsibilities with respect to plant security and, therefore, the need for high assurance that they are trustworthy and reliable.
	(b)(1)(iv) The licensee's, applicant's, or C/V's reviewing official.	Proposed § 73.56(b)(1)(iv) would introduce a new term, "reviewing official," to § 73.56 to refer to an individual who is designated by a licensee, applicant, or C/V to be responsible for reviewing and evaluating information about persons who are applying for unescorted access authorization and determining whether to grant, deny, maintain, or unfavorably terminate unescorted access authorization. The proposed paragraph would require reviewing officials to be subject to the AA program because of the key role these individuals play in providing high assurance that persons who are granted unescorted access to protected areas and electronic access to operational safety, security, or emergency response systems within protected or vital areas are trustworthy and reliable.

		In addition, reviewing officials' actions affect the confidence that the public, management, the NRC, and individuals who are subject to the AA program have in the integrity of the program and the accuracy and reliability of the authorization decisions that are made under the program. Therefore, the NRC believes that reviewing officials must meet the highest standards for trustworthiness and reliability, including the requirements of an AA program.
	(b)(2) At the licensee's, applicant's, or C/V's discretion, other individuals who are designated in access authorization program procedures may be subject to an authorization program that meets the requirements of this section.	Proposed § 73.56(b)(2) would recognize the long-standing industry practice, which has been endorsed by the NRC, of subjecting additional individuals to authorization requirements during periods when those individuals do not require and have not been granted unescorted access to protected or vital areas. For example, some C/Vs, whose personnel may be called upon by a licensee to work at a licensee's site under contract, implement full authorization programs to cover those personnel. Similarly, some licensees require employees who are normally stationed at their corporate headquarters to be subject to an authorization program, for such access, is referred to as having "unescorted access" (UA).

		The proposed paragraph would be added to give licensees, applicants, and C/Vs who implement authorization programs that meet the requirements of this part the authority to do so under the proposed rule.
§ 73.56(b) *General performance objective and requirements.* (1) The licensee shall establish and maintain an access authorization program granting individuals unescorted access to protected and vital areas with the objective of providing high assurance that individuals granted unescorted access are trustworthy and reliable, and do not constitute an unreasonable risk to the health and safety of the public including a potential to commit radiological sabotage.	(c) General performance objective. Access authorization programs must provide high assurance that the individuals who are specified in paragraph (b)(1) of this section, and, if applicable, (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.	Proposed § 73.56(c) would retain the meaning of the current program performance objective, which is embedded in current § 73.56(b), but would separate it from the requirement in the current paragraph for licensees to establish and maintain an AA program. The requirement to establish and maintain AA programs would be moved to proposed § 73.56(a), where it would be imposed on each entity who would be subject to the section, for organizational clarity. The performance objective would be revised to add cross-references to the categories of individuals who must be subject to an authorization program, as specified in proposed § 73.56(b), because the proposed rule would require that certain individuals, in addition to those who have unescorted physical access to protected and vital areas of a nuclear power plant, would be subject to the AA program, as discussed with respect to § 73.56(b).

		In addition, the phrase, “common defense and security,” would be added to the proposed paragraph to convey the purpose of authorization programs more specifically, which would include protection of the public from the potential insider activities defined in current § 73.1(a)(1)(B) and (a)(2)(B).
§ 73.56(2) Except as provided for in paragraphs (c) and (d) of this section, the unescorted access authorization program must include the following: (i) A background investigation designed to identify past actions which are indicative of an individual's future reliability within a protected or vital area of a nuclear power reactor. As a minimum, the background investigation must verify an individual’s...	(d) Background investigation. In order to grant unescorted access authorization to an individual, the licensees, applicants and C/Vs specified in paragraph (a) of this section shall ensure that the individual has been subject to a background investigation. The background investigation must include, but is not limited to, the following elements:	Proposed § 73.56(d) would amend current § 73.56(b)(2)(i), which requires authorization programs to include a background investigation and describes the aspects of an individual’s background to be investigated. Proposed § 73.56(d) would retain the requirements of the current paragraph, but increase the level of detail with which they are specified in response to implementation questions from licensees and in order to increase consistency among authorization programs, as discussed in Section IV.3. Because the requirements in the proposed rule would be more detailed, the current paragraph would be restructured and subdivided to present requirements for each element of the background investigation in a separate paragraph. This change would be made for increased clarity in the organization of the rule. The cross-references to paragraphs (c) and (d) in the current provision would be deleted because they would no longer apply in the reorganized section.

		The proposed provision would use the phrase, "ensure that the individual has been subject to a background investigation," because completion of every element of a background investigation may not be required each time an individual applies for UAA. As discussed with respect to proposed § 73.46(h)(1) and (h)(2), the proposed rule would permit licensees, applicants, and C/Vs, in order to meet the requirements of this section, to accept and rely on certain background investigation elements, psychological assessments, and behavioral observation training conducted by other licensees, applicants, and C/Vs who are subject this section. This permission would reduce unnecessary regulatory burden by eliminating redundancies in authorization program elements that cover the same subject matter and periods of time. However, as discussed with respect to proposed paragraphs (h) and (i)(1) of this section, the proposed rule would establish time limits on the permission to accept and rely on authorization program elements to which the individual was previously subject, based upon how far in the past the background investigation element, psychological assessment, and behavioral observation training was conducted.

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

		Proposed § 73.56(o)(6) would further require the licensee, applicant, or C/V to ensure that any necessary corrections are made to information about the individual that has been recorded in the information-sharing mechanism that would be required under proposed § 73.56(o)(6), as discussed with respect to that paragraph. These are also industry practices that have been endorsed by the NRC and incorporated into licensees' Physical Security Plans. Permitting the individual to review and have the opportunity to correct personal information that is collected about him or her is necessary to maintain individuals' confidence in the fairness of authorization programs by protecting individuals from possible adverse employment actions that may result from an inability to gain unescorted access to protected areas, based upon incorrect information. Requiring the entities who are subject to this section to correct information contained in the information-sharing mechanism, as would be required under proposed § 73.56(o)(6), is necessary to maintain the integrity of the personal information shared among the entities who would be subject to the proposed section, and the effectiveness of AA programs.

	(d)(1)(i) The subject individual may withdraw his or her consent at any time. The licensee, applicant or C/V to whom the individual has applied for unescorted access authorization shall inform the individual that — (A) Withdrawal of his or her consent will withdraw the individual's current application for access authorization under the licensee's, applicant's or C/V's authorization program; and (B) Other licensees, applicants and C/Vs will have access to information documenting the withdrawal through the information-sharing mechanism required under paragraph (o)(6) of this section.	Proposed § 73.56(d)(1)(i) would specify that an individual who has given his or her written consent for a background investigation under proposed § 73.56(d)(1) may withdraw that consent at any time. However, because a background investigation is one of the requirements for granting UAA, and because the background investigation cannot be completed without the subject individual's consent, proposed § 73.56(d)(1)(i)(A) would specify that the licensee, applicant, or C/V to whom the individual has applied for UAA must inform the individual who has withdrawn consent that withdrawal of consent will terminate the individual's current application for UAA. In addition, the licensee, applicant, or C/V would be required by proposed § 73.56(d)(1)(i)(B) to notify the individual that other licensees, applicants, and C/Vs will have access to information documenting the withdrawal through the information-sharing mechanism required under proposed § 73.56(o)(6). That proposed paragraph would require that information specified in the licensee's or applicant's Physical Security Plan about individuals who have applied for UAA, must be recorded and retained in a database that is administered as an information-sharing mechanism by licensees and applicants subject to § 73.56.

	(d)(1)(ii) If an individual withdraws his or her consent, the licensees, applicants and C/Vs specified in paragraph (a) of this section 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. In the information-sharing mechanism required under paragraph (o)(6) of this section, the licensee, applicant, or C/V shall record the individual's application for unescorted access authorization; his or her withdrawal of consent for the background investigation; the reason given by the individual for the withdrawal, if any; and any pertinent information collected from the background investigation elements that were completed.	Proposed § 73.56(d)(1)(ii) would establish several requirements related to a withdrawal of consent by an individual who has applied for UAA. The proposed paragraph would require the entities who are subject to this section to document the individual's withdrawal of consent, and complete and document any elements of the background investigation that had been initiated before the time at which an individual withdraws his or her consent, and would prohibit the initiation of any element that was not in progress. For example, if a licensee had submitted a request to a credit history reporting agency before an individual withdrew his or her consent, the proposed paragraph would require the licensee to document the credit history information that is obtained about the individual, even if the licensee receives the credit history report after the date on which the individual withdrew his or her consent. However, if the licensee had not yet requested information about the individual's military service history at the time the individual withdraws consent, the proposed provision would prohibit the licensee from initiating a request for military service history information. There are many reasons that an individual may withdraw his or her consent for the background investigation.

		In most instances, the reason that an individual withdraws his or her consent is legitimate, such as a change in the individual's work assignment. However, in some instances, the NRC is aware that individuals have withdrawn consent for the background investigation in order to attempt to prevent the discovery of adverse information or the sharing of adverse information already discovered about the individual by the licensee with other licensees. If the licensee were to stop all information gathering at the time at which the individual withdrew his or her consent, the likelihood that the adverse information would be discovered would be reduced. As a result, the individual could be afforded an opportunity to create a risk to public health and safety and the common defense and security by having physical access to a protected or vital area, and most importantly, be in a position to observe the licensee's security posture by obtaining access to a licensee facility under escort, because a rigorous background investigation is not required for individuals who "visit" a nuclear power plant under escort.

		Similarly, if information that had been requested by the licensee, such as a criminal history report under proposed § 73.57 [Requirements for criminal history checks of individuals granted unescorted access to a nuclear power facility or access to safeguards information by power reactor licensees] of this chapter or the credit history report under proposed § 73.56(d)(5), was received by the licensee after the time the individual withdrew consent and contained adverse information, but that adverse information was not documented in the information-sharing mechanism required under proposed paragraph (o)(6) of this section, the individual also could be inappropriately permitted to visit under escort the same or another site because the adverse information would not be available for review. Therefore, the proposed provisions would be necessary to maintain the effectiveness of AA programs in protecting public health and safety and the common defense and security by ensuring that all available information about individuals who have applied for UAA is documented and shared, while also protecting the privacy rights of individuals by initiating no further elements of the background investigation when an individual withdraws his or her consent.

		The proposed paragraph would also require licensees, applicants, and C/Vs to create a record, accessible to other licensees, applicants, and C/Vs, of the fact that an individual withdrew his or her consent to the background investigation and the reason for the withdrawal. This record would need to be created in the information-sharing mechanism required by proposed § 73.56(o)(6), in order for licensees, applicants, and C/Vs to carry out the notice requirement in proposed § 73.56(d)(1)(i)(B).
§ 73.56(4) Failure by an individual to report any previous suspension, revocation, or denial of unescorted access to nuclear power reactors is considered sufficient cause for denial of unescorted access authorization.	(d)(1)(iii) The licensees, applicants, and C/Vs specified in paragraph (a) of this section shall inform, in writing, any individual who is applying for unescorted access authorization that the following actions related to providing and sharing the personal information under this section are sufficient cause for denial or unfavorable termination of unescorted access authorization: (A) Refusal to provide written 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 authorization;	Proposed § 73.56(d)(1)(iii) would replace current § 73.56(b)(4). The proposed paragraph would retain the intent of the current provision in proposed § 73.56(d)(4), but would add other actions related to providing and sharing personal information that would be sufficient cause for a reviewing official to deny or unfavorably terminate an individual's UAA. Proposed paragraph (d)(1)(iii)(B) of this section would add falsification of any personal history information as a sufficient reason to deny or unfavorably terminate UAA in order to deter falsification attempts.

	(C) Refusal to provide written consent for the sharing of personal information with other licensees, applicants, or C/Vs required under paragraph (d)(4)(v) of this section; and (D) Failure to report any arrests or formal actions specified in paragraph (g) of this section.	Proposed paragraph (d)(1)(iii)(D) of this section would add failure to comply with the arrest-reporting requirements of proposed paragraph (g) of this section as a sufficient reason to deny or unfavorably terminate UAA in order to deter individuals from delaying or failing to report such incidents. The additional actions that would be sufficient cause for denial or unfavorable termination would include: refusing to provide written consent for the background investigation that would be required under proposed paragraph (d)(1)(iii)(A) of this section; refusing to provide personal history information required under paragraph (d)(2) of this section, in proposed (d)(1)(iii)(B); and refusing to provide written consent for the individual's personal information to be shared among the entities who would be subject to this section that would be required under paragraph (d)(4)(v) of this section, in proposed paragraph (d)(1)(iii)(C).

		The proposed rule would specify these requirements for the disclosure and sharing of personal information because implementation of the AA programs required under this section requires individuals to disclose and permit the sharing of such personal information, subject to the protections of such information that would be provided in proposed § 73.56(m). The proposed paragraph would also require the entities who are subject to this section to inform individuals of the potential consequences of these actions so that individuals understand the requirements to which they are subject and, therefore, would be more likely to comply with them. The proposed paragraph would delete the terms, “suspension” and “revocation,” and replace them with the term, “unfavorable termination.” Historically, there have been some inconsistencies between § 73.56 access authorization requirements and related requirements in 10 CFR part 26 that have led to implementation questions from licensees, as well as inconsistencies in how the licensees have implemented the requirements.

		During the public meetings discussed in Section IV.3, the stakeholders provided examples of ambiguities in the terms used in § 73.56 and how these ambiguities and lack of clarity in § 73.56 had resulted in unintended consequences. Therefore, to address stakeholder requests for clarity and consistently describe the actions of denying UAA to an individual and terminating an individual's UAA for cause in proposed § 73.56, only the terms, "deny or denial" and "unfavorably terminate or unfavorable termination," would be used in the proposed paragraph and throughout the proposed section.
	(d)(2) Personal history disclosure. (i) Any individual who is applying for unescorted access authorization shall disclose the personal history information that is required by the licensee's, applicant's, or C/V's authorization program and any information that may be necessary for the reviewing official to make a determination of the individual's trustworthiness and reliability.	Proposed § 73.56(d)(2) would require an individual who is applying for UAA to provide the personal information that is required under the licensee's, applicant's, or C/V's authorization program, and any information that may be necessary for the reviewing official to evaluate the individual's trustworthiness and reliability. The proposed provision would be added to impose a requirement on individuals to divulge personal information in order to be granted UAA, in response to stakeholder requests at the public meetings discussed in Section IV.3.

		The proposed paragraph would not specify the nature of the information that individuals may be required to disclose because the information may vary widely, depending upon a number of factors, including, but not limited to, whether or not the individual has previously held UAA; the length of time that has elapsed since his or her last period of UAA was terminated; the job duties and responsibilities that the individual would perform for which UAA is required; and whether any adverse information about the individual is disclosed or discovered as a result of the background investigation, psychological assessment, or the suitable inquiry and drug and alcohol testing required under part 26 of this chapter. Although the amount and nature of information to be disclosed would vary depending on the factors described, individuals applying for UAA would be required to disclose some personal history information each time he or she applies for UAA, as discussed with respect to proposed § 73.56(h) [Granting unescorted access authorization].

	(d)(2)(ii) Licensees, applicants, and C/Vs may not require an individual to disclose an administrative withdrawal of unescorted access authorization under the requirements of paragraphs (g), (h)(7), or (i)(1)(v) of this section, if the individual's unescorted access authorization was not subsequently denied or terminated unfavorably by a licensee, applicant, or C/V.	Proposed § 73.56(d)(2)(ii) would prohibit a licensee, applicant, or C/V from requiring an individual to report an administrative withdrawal of UAA that may be required under proposed § 73.56(g), (h)(7), or (i)(1)(v), except if the information developed or discovered about the individual during the period of the administrative withdrawal resulted in a denial or unfavorable termination of the individual's UAA. The proposed paragraph would ensure that a temporary administrative withdrawal of an individual's UAA, caused by an administrative delay in completing an evaluation of any formal legal action, or any portion of a background investigation, re-investigation, or psychological assessment or re-assessment that is not under the individual's control, would not be treated as an unfavorable termination, except if the reviewing official determines that the delayed information requires denial or unfavorable termination of the individual's UAA. This proposed provision would be necessary to maintain the public's and individuals' confidence in the fairness of AA programs by protecting individuals from possible adverse employment actions that may be based upon administrative delays for which they are not responsible.

§ 73.56(b)(2)(i)... true identity, and develop information concerning an individual's employment history, education history, credit history, criminal history, military service, and verify an individual's character and reputation.	(d)(3) Verification of true identity. Licensees, applicants, and C/Vs shall verify the true identity of an individual who is applying for 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 C/Vs shall validate the social security number that the individual has provided, and, in the case of foreign nationals, the alien registration number that the individual provides. In addition, licensees, applicants, and C/Vs shall also determine whether the results of the fingerprinting required under § 73.21 confirm the individual's claimed identity, if such results are available.	Proposed § 73.56(d)(3) would expand on the portion of current § 73.56(b)(2)(i) that requires licensees to verify an individual's true identity. The proposed paragraph would require the entities who are subject to this section, at a minimum, to validate the social security number, or in the case of foreign nationals, the alien registration number, that the individual has provided to the licensee, applicant or C/V. The term, "validation," would be used in the proposed paragraph to indicate that licensees, applicants and C/Vs would be required to take steps to access information in addition to that provided by the individual from other reliable sources to ensure that the personal identifying information the individual has provided to the licensee is authentic. This validation could be achieved through a variety of means, including, but not limited to, accessing information from databases that are maintained by the Federal Government, or evaluating an accumulation of information, such as comparing the social security number the individual provided to the social security number(s) included in a credit history report and information obtained from other sources.

		The proposed paragraph would also require using the information obtained from fingerprinting individuals, as required under proposed § 73.21, to confirm an individual's identity, if that information is available. The proposed requirement clarifies the NRC's intent with respect to this portion of the background investigation.
§ 73.56(b)(2)(i)...and develop information concerning an individual's employment history...	(d)(4) Employment history evaluation. Licensees, applicants, and C/Vs shall ensure that an employment history evaluation has been completed, by questioning the individual's present and former employers, and by determining the activities of individuals while unemployed.	Proposed § 73.56(d)(4) would amend the portion of current § 73.56(b)(2)(i) that requires licensees to develop information concerning an individual's employment history, education history, and military service. This paragraph would be added in response to many implementation questions about these requirements from licensees. Because the proposed paragraph would add several clarifications of the current requirements, it would be subdivided to present each requirement separately for organizational clarity in the rule. Considered together, the requirements of proposed § 73.56(d)(4) would clarify the NRC's intent that periods of unemployment, education, and military service must be evaluated only if the individual claims them instead of typical civilian employment.

		Proposed § 73.56(d)(4) would require licensees, applicants, and C/Vs to demonstrate a best effort to complete the employment history evaluation. The term, “best effort,” would be added to clarify the requirements and increase consistency between § 73.56 and related requirements in 10 CFR 26.27(a). The best effort criterion recognizes licensees’, applicants’, and C/Vs’ status as commercial entities with no legal authority to require the release of the information from other private employers and educational institutions. Because of privacy and potential litigation concerns, some private employers and educational institutions may be unable or unwilling to release qualitative information about a former employee or student. Therefore, the best effort criterion would first require licensees, applicants, and C/Vs to seek employment information from the primary source (e.g., a company, private employer, or educational institution that the applicant has listed on his or her employment history), but recognizes that it may not be forthcoming. In this case a licensee, applicant, or C/V would be required to seek information from an alternate, secondary source when the information from the primary source is unavailable.

		The proposed provision would use the phrase, “ensure that the employment history evaluation has been completed,” because a licensee, applicant, or C/V may not be required to conduct an employment history evaluation for every individual who applies for UAA. As discussed with respect to proposed § 73.56(h)(3) and (h)(4), the proposed rule would permit licensees, applicants, and C/Vs to accept and rely on elements of the background investigations, psychological assessments, and behavioral observation training conducted by other entities who are subject to this section to meet the requirements of this section. Therefore, the need for and extent of the employment history evaluation would vary, depending upon how much recent information was available to the licensee, applicant, or C/V from any previous periods during which the individual may have held UAA. In the case of individuals whose UAA has been interrupted for 30 or fewer days, proposed § 73.56(h) would not require an employment history evaluation for the reasons discussed with respect to that paragraph.

		However, proposed § 73.56(h) would establish time limits on the permission to accept and rely on AA program elements to which the individual was previously subject, based upon how far in the past the background investigation, psychological assessment, and behavioral observation training elements were completed. These time limits are discussed in more detail with respect to the specific provisions in the proposed rule that address them. The proposed provision would also require licensees, applicants, and C/Vs to determine the activities of individuals during periods in which the individual was unemployed. The proposed rule would add this requirement to make certain that, during the periods that individuals claim to have been unemployed, (1) they were not engaged in activities that may reflect adversely on their trustworthiness and reliability, such as confinement for periods of incarceration or in-patient drug or alcohol treatment, or (2) they intentionally failed to disclose periods of employment that were ended unfavorably.

	(d)(4)(i) For the claimed employment period, the employment history evaluation must ascertain the reason for termination, eligibility for rehire, and other information that could reflect on the individual's trustworthiness and reliability.	A new § 73.56(d)(4)(i) would specify the purpose of the employment history evaluation, which would be to ascertain information about the individual's trustworthiness and reliability, and the types of information that the licensee, applicant, or C/V would seek from employers regarding an individual who is applying for UAA. The proposed paragraph would require the entities who are subject to this section to ascertain, consistent with the "best effort" criterion established in proposed § 73.56(d)(4), the reason that the individual's employment was terminated, his or her eligibility for rehire, and other information that could reflect on the individual's trustworthiness and reliability. The term, "ascertain," would be used in the proposed paragraph because it is consistent with the terminology used by the industry to refer to the actions taken with respect to conducting the employment history evaluation and would, therefore, improve the clarity of this requirement for those who must implement it.

		In addition, there may be instances in which it is unnecessary for a licensee, applicant, or C/V to conduct the employment history evaluation, as discussed with respect to proposed § 73.56(d)(4), because proposed § 73.56(h)(2) would permit the entities who implement authorization programs to rely on employment history evaluations conducted by other entities who are subject to this section. In such cases, the licensee's, applicant's, or C/V's reviewing official would not review information that was developed under his or her AA program, but would ascertain the subject individual's employment history by reviewing information that had been collected by others. The proposed requirement would be added in response to implementation questions that have arisen about the employment history check that is required in current § 73.56(b)(2)(i).

§ 73.56(b)(2)(i)... the background investigation must ... develop information concerning an individual's ... military service...	(d)(4)(ii) If the claimed employment was military service, the licensee, applicant, or C/V who is conducting the employment history evaluation shall request a characterization of service, reason for separation, and any disciplinary actions that could affect a trustworthiness and reliability determination.	Proposed § 73.56(d)(4)(ii) would amend the portion of current § 73.56(2)(i) that requires licensees to develop information about an individual's military service. The proposed paragraph would clarify the NRC's intent that verification and characterization of the individual's military service would be required only if the individual claims military service as employment within the periods during which the individual would be required to disclose his or her employment history, as specified in proposed § 73.56(h) [Granting unescorted access authorization]. This clarification would respond to implementation questions from licensees and stakeholder requests at the public meetings discussed in Section IV.3.
§ 73.56(b)(2)(i)...and develop information concerning an individual's ... education history,....	(d)(4)(iii) Periods of self-employment or unemployment may be verified by any reasonable method. If education is claimed in lieu of employment, the licensee, applicant, or C/V shall request information that could reflect on the individual's trustworthiness and reliability and, at a minimum, verify that the individual was actively participating in the educational process during the claimed period.	Proposed § 73.56(d)(4)(iii) would be added at the request of stakeholders at the public meetings discussed in Section IV.3 to clarify the NRC's intent with respect to periods of self-employment, unemployment, or education, if the individual claims such activities within the periods during which the individual would be required to disclose his or her employment history, as specified in proposed § 73.56(h).

		The proposed paragraph would permit licensees, applicants, and C/Vs to use any reasonable means, consistent with the "best effort" criterion discussed with respect to proposed § 73.56(d)(4), to verify the individual's activities during claimed periods of self-employment and unemployment. Reasonable means to verify the individual's activities may include, but would not be limited to, a review of business or tax records documenting the individual's self-employment, copies of unemployment compensation checks, or interviews with business associates or acquaintances. To verify education in lieu of employment, the proposed paragraph would require the entities who are subject to this section to request information from the claimed educational institution that could reflect on the individual's trustworthiness and reliability. However, for reasons that are similar to those discussed with respect to proposed § 73.56(d)(4), the NRC recognizes that it may be difficult to obtain information from an educational institution about the individual's behavior while a student. Therefore, the proposed paragraph would permit licensees, applicants, and C/Vs to verify, at a minimum, that the applicant was attending and actively participating in school during the claimed period(s).

	(d)(4)(iv) If a company, previous employer, or educational institution to whom the licensee, applicant, or C/V has directed a request for information refuses to provide information or indicates an inability or unwillingness to provide information within 3 business days of the request, the licensee, applicant, or C/V shall document this refusal, inability, or unwillingness in the licensee's, applicant's, or C/V's record of the investigation, and obtain a confirmation of employment or educational enrollment and attendance from at least one alternate source, with questions answered to the best of the alternate source's ability. This alternate source may not have been previously used by the licensee, applicant, or C/V to obtain information about the individual's character and reputation. If the licensee, applicant, or C/V uses an alternate source because employment information is not forthcoming within 3 business days of the request, the licensee, applicant, or C/V need not delay granting unescorted access authorization to wait for any employer response, but shall evaluate and document the response if it is received.	Proposed § 73.56(d)(4)(iv) would further clarify the NRC's intent with respect to the actions that licensees, applicants, and C/Vs would take to meet the best effort criterion in proposed § 73.56(d)(4), in response to many implementation questions received from licensees. The proposed paragraph would address circumstances in which a primary source of information refuses to provide employment information or indicates an inability or unwillingness to provide it within 3 days of the request. Licensees and other entities would be required to document that the request for information was directed to the primary source and the nature of the response (i.e., a refusal, inability, or unwillingness). If a licensee, applicant, or C/V encounters such circumstances, the proposed paragraph would require the licensee, applicant, permit, or C/V to seek employment history information from an alternate source, to the extent of the alternate source's ability to provide the information. An alternate source may include, but would not be limited to, a co-worker or supervisor at the same company who had personal knowledge of the applicant, if such an individual could be located.

		However, the proposed rule would prohibit the licensee, applicant, or C/V from using the alternate source of employment information to meet the requirements in proposed § 73.56(d)(6) for a character reference, in order to ensure that the scope of the background investigation is sufficiently broad to provide high assurance that individuals who are granted UAA are trustworthy and reliable. The proposed paragraph would permit licensees and other entities to grant UAA, if warranted, when a response has been obtained from an alternate source, without waiting more than 3 days after the request for information was directed to a primary source. The 3-day period would be established because industry and NRC experience in implementing current § 73.56 has shown that if an employer or educational institution intends to respond to the request for information, the response will be forthcoming within this period. Therefore, there is no added benefit to public health and safety or the common defense and security in requiring licensees, applicants, or C/Vs to wait longer than 3 days before implementing the alternative methods of meeting the employment history evaluation requirements that would be permitted in the proposed paragraph.

		However, should the licensee, applicant, or C/V receive an employer response to the request for information after the 3-day period, the proposed paragraph would require that the implications of the information must be evaluated with respect to the individual's trustworthiness and reliability and the information documented, so that it is available to other licensees, applicants, and C/Vs. These changes would be made to reduce unnecessary regulatory burden while maintaining high assurance that individuals who are subject to an AA program are trustworthy and reliable.

	(d)(4)(v) When any licensee, applicant, or C/V specified in paragraph (a) of this section is legitimately seeking the information required for an unescorted access authorization decision under this section and has obtained a signed release from the subject individual authorizing the disclosure of such information, a licensee, applicant, or C/V who is subject to this section shall disclose whether the subject individual's unescorted access authorization was denied or terminated unfavorably. The licensee, applicant, or C/V who receives the request for information shall make available the information upon which the denial or unfavorable termination of unescorted access authorization was based.	Proposed § 73.56(d)(v) would require licensees, applicants, and C/Vs who are subject to this section to share employment history information that they have collected, if contacted by another licensee, applicant, or C/V who has a release signed by the individual who is applying for UAA that would permit the sharing of that information. This proposed provision would amend the requirement to release employment history information in current § 73.56(f)(2) and would be consistent with related requirements in 10 CFR Part 26. The proposed provision would also clarify that the information must also be released to C/Vs who have authorization to programs when the C/V has obtained the required signed release from the applicant. This proposed clarification is necessary because some licensees have misinterpreted current § 73.56(f)(2) as prohibiting the release of employment history information to C/Vs who administer authorization programs under this section. These requirements are necessary to ensure that adequate information to serve as a basis for UAA decisions can be obtained by a licensee, applicant, or C/V.

	(d)(4)(vi) In conducting an employment history evaluation, the licensee, applicant, or C/V may obtain information and documents by electronic means, including, but not limited to, telephone, facsimile, or email. The licensee, applicant, or C/V shall make a record of the contents of the telephone call and shall retain that record, and any documents or files obtained electronically, in accordance with paragraph (o) of this section.	Proposed § 73.56(d)(4)(vi) would permit licensees, applicants, and C/Vs to use electronic means of obtaining the employment history information to increase the efficiency with which licensees, applicants, and C/V could obtain the employment history information. The proposed paragraph would be added in response to stakeholder requests at the public meetings discussed in Section IV.3, and would be consistent with related requirements in 10 CFR Part 26. The proposed paragraph would also add a cross-reference to the applicable records retention requirement in proposed § 73.56(o) [Records] to ensure that licensees, applicants, and C/Vs are aware of the applicability of these requirements to the employment history information obtained electronically.

§ 73.56(b)(2)(i)...and develop information concerning an individual's... credit history, ...	(d)(5) Credit history evaluation. The licensees, applicants, and C/Vs specified in paragraph (a) of this section shall ensure that the full credit history of any individual who is applying for unescorted access authorization has been evaluated. A full credit history evaluation must include, but would not be 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.	Proposed § 73.56(d)(5) would retain the requirement for a credit history evaluation that is embedded in current § 73.56(b)(2)(i) and provide more detailed requirements, in response to stakeholder requests at the public meetings discussed in Section IV.3. The proposed paragraph would require the credit history evaluation to include an inquiry to detect any past instances of fraud or misuse of social security numbers or other financial identifiers. This requirement would be added because most credit-reporting agencies require a specific request for this information before they report it, and the NRC has determined that instances of fraud or misuse of financial identifiers, such as social security numbers or the names that an individual has used, may provide important information about an individual's trustworthiness and reliability. The proposed paragraph would also require the entities who are subject to this section to review all of the information that is provided by the national credit-reporting agency, as part of the background investigation process.

		The proposed paragraph would use the term, “full” to convey that there is no time limit on the number of years of credit history information that the reviewing official would consider or other limitations on using information contained in the credit history report to assist in determining the individual’s trustworthiness and reliability. In the past, licensees’ AA program procedures limited the number of years of the individual’s credit history that reviewing officials were required to consider in determining an individual’s trustworthiness and reliability. As a result, some reviewing officials may not have considered credit history information for several years, even if the reporting agency provided it. As a result, individuals who were subject to different authorization programs were evaluated inconsistently. Furthermore, credit history reporting agencies also provide employment data that can be compared to the information disclosed by the applicant for UAA to validate the individual’s disclosure. However, some AA program procedures did not require the reviewing official to make this comparison.

		Therefore, the proposed paragraph would require the reviewing official to consider the “full” credit history report, in order to strengthen the effectiveness of the credit history evaluation element of AA programs and increase the consistency with which licensees, applicants, and C/Vs would conduct the credit history evaluation.

§ 73.56(b)(2)(i)...and develop information concerning an individual's... character and reputation.	(d)(6) Character and reputation. The licensees, applicants, and C/Vs specified in paragraph (a) of this section shall ascertain the character and reputation of an individual who has applied for 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.	Proposed § 73.56(d)(6) would expand on the requirement in current § 73.56(b)(2)(i) for licensees to verify an individual's character and reputation. The proposed provision would require the entities who implement AA programs to develop information about an individual's trustworthiness and reliability by contacting and interviewing associates of the individual who would have knowledge of his or her character and reputation, but who would not be a member of the individual's immediate family or reside in his or her household. Family and household members would be excluded because these individuals are typically reluctant to reveal any adverse information, if it exists. The term, "ascertain," would replace "verify," in the proposed paragraph because it is consistent with the terminology used by the industry to refer to the actions taken with respect to determining an individual's character and reputation and would, therefore, improve the clarity of this requirement for those who must implement it.

		In addition, there would be instances in which it is unnecessary for a licensee, applicant, or C/V to conduct the character and reputation evaluation because proposed § 73.56(h)(4) would permit the entities who implement AA programs to rely on the background investigations conducted by other entities who are subject to this section. In such cases, the licensee's, applicant's, or C/V's reviewing official would not review information that was collected under his or her AA program, but would ascertain the subject individual's character and reputation by reviewing information that had been collected by others. The last sentence of the proposed paragraph would clarify that the scope of the reference checks would be limited to developing information that would be useful to the reviewing official in determining the individual's trustworthiness and reliability for the UAA decision. This requirement would be added in response to stakeholder requests at the public meetings discussed in Section IV.3 for increased clarity and specificity in the regulation's requirements.

§ 73.56(b)(2)(i)...and develop information concerning an individual's... criminal history...	(d)(7) Criminal history review. The licensee's, applicant's, or C/V's reviewing official shall evaluate the entire criminal history record of an individual who is applying for unescorted access authorization to assist in determining whether the individual has a record of criminal activity that may adversely impact his or her trustworthiness and reliability. The criminal history record must be obtained in accordance with the requirements of § 73.57.	Proposed § 73.56(d)(7) would amend the requirement in current § 73.56(b)(2)(i) for licensees to develop information about an individual's criminal history. The proposed provision would eliminate the current requirement to develop criminal history information because proposed § 73.57 [Requirements for criminal history checks of individuals granted unescorted access to a nuclear power facility or access to Safeguards Information by power reactor licensees] would establish the methods by which criminal history information about individuals who are applying for UAA would be obtained and it is unnecessary to repeat those requirements in this section. The proposed paragraph would require the reviewing official to review the individual's entire criminal history record. This requirement would be necessary because, in the past, some licensees limited the criminal history review to the individual's history over the past 5 or fewer years, but did not consider criminal history information from earlier years, even if the reporting agency provided it. However, the NRC has determined that a review of all of the criminal history information that is provided in a criminal history record provides higher assurance that any instances or patterns of lawlessness are considered when determining whether an individual is trustworthy and reliable.

		Therefore, the proposed rule would incorporate this requirement in order to strengthen the effectiveness of AA programs.

§ 73.56(d) Requirements during cold shutdown. (1) The licensee may grant unescorted access during cold shutdown to an individual who does not possess an access authorization granted in accordance with paragraph (b) of this section provided the licensee develops and incorporates into its Physical Security Plan measures to be taken to ensure that the functional capability of equipment in areas for which the access authorization requirement has been relaxed has not been impaired by relaxation of that requirement. (2) Prior to incorporating such measures into its Physical Security Plan the licensee shall submit those plan changes to the NRC for review and approval pursuant to § 50.90. (3) Any provisions in licensees' security plans that allow for relaxation of access authorization requirements during cold shutdown are superseded by this rule. Provisions in licensees' Physical Security Plans on April 25, 1991 that provide for devitalization (that is, a change from vital to protected area status) during cold shutdown are not affected.	Deleted.	Current § 73.56(d) [Requirements during cold shutdown] would be eliminated from the proposed rule. Because of an increased concern with a potential insider threat, as discussed in Section IV.3, the NRC has determined that the relaxation of UAA requirements permitted in the current provision does not meet the Commission's objective of providing high assurance that individuals who have unescorted access to protected areas in nuclear power plants are trustworthy and reliable. Therefore, the current permission to grant unescorted access to an individual without meeting all of the requirements of proposed § 73.56 would be eliminated from the proposed rule. Licensees and applicants would continue to be permitted to seek an exemption from the requirements of proposed § 73.56 under current § 73.5 [Specific exemptions].

§ 73.56(b)(2)(ii) A psychological assessment designed to evaluate the possible impact of any noted psychological characteristics which may have a bearing on trustworthiness and reliability.	(e) Psychological assessment. In order to assist in determining an individual's trustworthiness and reliability, the licensees, applicants, and C/Vs specified in paragraph (a) of this section shall ensure that a psychological assessment has been completed of the individual who is applying for unescorted access authorization. The psychological assessment must be designed to evaluate the possible adverse impact of any noted psychological characteristics on the individual's trustworthiness and reliability.	Proposed § 73.56(e) would amend current § 73.56(b)(2)(ii), which requires AA programs to include a psychological assessment, by adding several requirements to the current rule. Because the requirements in the proposed rule would be more detailed, the current paragraph would be restructured and subdivided to present the new requirements in separate paragraphs. This change would be made for increased clarity in the organization of the rule. The proposed paragraph would retain the current requirement for the psychological assessment to be designed to evaluate the implications of the individual's psychological characteristics on his or her trustworthiness and reliability in a separate sentence for clarity. For the same reason, "adverse" would be added to more clearly describe the intended purpose of the psychological assessment. The proposed provision would retain the intent of the current requirement for AA programs to include a psychological assessment, but would use the phrase, "has been completed," because licensees, applicants, and C/Vs may not be required to complete the psychological assessment each time that an individual applies for UAA.

		As discussed with respect to proposed § 73.56(h)(1), AA programs would be permitted to rely on psychological assessments that were completed by other AA programs. Individuals who have been subject to a psychological assessment, which was conducted in accordance with requirements of this proposed section and resulted in the granting of UAA, within the time period specified in the licensee's or applicant's Physical Security Plan [as discussed with respect to proposed § 73.56(i)(1)(v)], would not be required to be assessed again in order to be granted UAA.
	(e)(1) A licensed clinical psychologist or psychiatrist shall conduct the psychological assessment.	Proposed § 73.56(e)(1) would establish minimum requirements for the credentials of individuals who perform the psychological assessments that are required under current § 73.56(b)(2)(ii), which are not addressed in the current rule. The proposed provision would require a licensed clinical psychologist or psychiatrist to conduct the psychological assessment, because the extensive education, training, and supervised clinical experience that these professionals must possess in order to be licensed under State laws would provide high assurance that they are qualified to conduct the psychological assessments that are required under the rule.

		The proposed rule would impose this new requirement because of the key role that the psychological assessment element of AA programs plays in assuring the public health and safety and common defense and security when determining whether an individual is trustworthy and reliable. Therefore, the proposed provision would be added to strengthen the effectiveness of AA programs.
	(e)(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.	A new § 73.56(e)(2) would require psychological assessments to be conducted in accordance with ethical principles for conducting such assessments that are established by the American Psychological Association or the American Psychiatric Association, as applicable. In order to meet State licensure requirements, clinical psychologists and psychiatrists are required to practice in accordance with the applicable professional standards. However, the proposed rule would add a reference to these professional standards to emphasize the importance that the NRC places on the proper conduct of psychological assessments, in order to ensure the rights of individuals, consistent treatment, and the effectiveness of the psychological assessment component of AA programs.

	(e)(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 implications for an individual's trustworthiness and reliability. Predetermined thresholds must be applied in interpreting the results of the psychological test, to determine whether an individual shall be interviewed by a psychiatrist or licensed clinical psychologist under paragraph (e)(4)(i) of this section.	Proposed § 73.56(e)(3) would establish new requirements for the psychological testing that licensees, applicants, and C/Vs would conduct as part of the psychological assessment. The proposed paragraph would require the administration and interpretation of an objective psychological test that provides information to aid in identifying personality disturbances and psychopathology. The proposed rule would specify psychological tests that are designed to identify indications of personality disturbances and psychopathology because some of these conditions may reflect adversely on an individual's trustworthiness and reliability. The proposed rule would not prohibit the use of other types of psychological tests, such as personality inventories and tests of abilities, in the psychological assessment process, but would establish the minimum requirement for a test that identifies indications of personality disturbances and psychopathology because the identification of these conditions is most relevant to the purpose of the psychological assessment element of AA programs. The proposed provision would also require the use of standardized, objective psychological tests to reduce potential variability in the testing that is conducted under this section.

		Decreasing potential variability in testing is important to provide greater assurance than in the past that individuals who are applying for or maintaining UAA are treated consistently under the proposed rule. The proposed rule would not prohibit the use of other types of psychological tests, such as projective tests, in the psychological assessment process, but would establish the minimum requirement for a standardized, objective test to facilitate the psychological re-assessments that would be required under proposed § 73.56(i)(1)(v). Comparing scores on a standardized, objective test to identify indications of any adverse changes in the individual's psychological status is simplified when the testing that is performed for a re-assessment is similar to or the same as previous testing that was conducted under this section, particularly when the clinician who conducts the re-assessment did not conduct the previous testing. The proposed paragraph would also require licensees, applicants, and C/Vs to establish thresholds in interpreting the results of the psychological test, to aid in determining whether an individual would be required to be interviewed by a psychiatrist or licensed clinical psychologist under proposed paragraph (e)(4)(ii) of this section.

		The NRC is aware of 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. Different clinical psychologists providing services to the same or different AA programs would vary in the thresholds they applied in determining whether an individual's test results indicated the need for further evaluation in a clinical interview. As a consequence, whether or not individuals who had the same patterns of scores on the psychological test would be subject to a clinical interview would vary both within and between AA programs. The proposed rule would add a requirement for predetermined thresholds to reduce this variability in order to protect the rights of individuals who are subject to AA programs to fair and consistent treatment.

	(e)(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 licensee's or applicant's Physical Security Plan requires a clinical interview based on job assignments.	A new § 73.56(e)(4) would establish requirements for the conditions under which the psychological assessment must include a clinical interview. Proposed § 73.56(e)(4)(i) would require a clinical interview if an individual's scores on the psychological test identified indications of disturbances in personality or psychopathology that would necessitate further assessment. The clinical interview would be performed by a licensed clinical psychologist or psychiatrist, consistent with the ethical principles for conducting psychological assessments that are established by the American Psychological Association or the American Psychiatric Association. The purposes of the clinical interview would include, but would not be limited to, validating the test results and assessing their implications for the individual's trustworthiness and reliability. Proposed § 73.56(e)(4)(ii) would also require a clinical interview for some individuals who would be identified in the licensee's or applicant's Physical Security Plan. In general, the individuals who would always receive a clinical interview before being granted UAA would be those who perform critical operational and security-related functions at the licensee's site.

		The proposed requirements are necessary to ensure that any noted psychological characteristics of individuals who are applying for or maintaining UAA do not adversely affect their trustworthiness and reliability.
	(e)(5) If, in the course of conducting the psychological assessment, the licensed clinical psychologist or psychiatrist identifies indications of, or information related to, a medical condition that could adversely impact the individual's fitness for duty or trustworthiness and reliability, the psychologist or psychiatrist shall inform the reviewing official, who shall ensure that an appropriate evaluation of the possible medical condition is conducted under the requirements of part 26 of this chapter.	A new § 73.56(e)(5) would require the psychologist or psychiatrist who conducts the psychological assessment to report to the reviewing official any information obtained through conducting the assessment that indicates the individual may have a medical condition that could adversely affect his or her fitness for duty or trustworthiness and reliability. For example, some psychological tests identify indications of a substance abuse problem. Or, an individual may disclose during the clinical interview that he or she is taking prescription medications that could cause impairment. In these instances, the proposed rule would require the reviewing official to ensure that the potential impact of any possible medical condition on the individual's fitness for duty or trustworthiness and reliability is evaluated. The term, "appropriate," would be used with respect to the medical evaluation to recognize that healthcare professionals vary in their qualifications.

		For example, a psychiatrist who conducts the assessment would be qualified to assess the potential impacts on an individual's fitness for duty of any psychoactive medications the individual may be taking, whereas a substance abuse professional, nurse practitioner, or other licensed physician may not. The NRC is aware of instances in which indications of a substance problem or other medical condition that could adversely affect an individual's fitness for duty or trustworthiness and reliability were identified during the psychological assessment, but were not communicated to fitness-for-duty program personnel and, therefore, were not evaluated as part of the access authorization decision. The proposed paragraph would be added to ensure that information about potential medical conditions is communicated and evaluated. This provision would be added to strengthen the effectiveness of the access authorization process.

§ 73.56(b)(2)(iii) Behavioral observation, conducted by supervisors and management personnel, designed to detect individual behavioral changes which, if left unattended, could lead to acts detrimental to the public health and safety.	(f) Behavioral observation. Access authorization programs must include a behavioral observation element that is designed to detect behaviors or activities that may constitute an unreasonable risk to the health and safety of the public and common defense and security, including a potential threat to commit radiological sabotage.	Proposed § 73.56(f) [Behavioral observation] would replace current § 73.56(b)(2)(iii), which requires licensees' AA programs to include a behavioral observation element, to be conducted by supervisors and management personnel, and designed to detect individual behavioral changes which, if left unattended, could lead to acts detrimental to the public health and safety. The proposed paragraph would amend the requirements of the current paragraph and add others. Proposed § 73.56(f) would amend the objective of the behavioral observation element of AA programs in the current provision. The proposed paragraph would eliminate the current reference to behavior changes which, if left unattended, could lead to detrimental acts. Although detecting and evaluating behavior changes in order to determine whether they may lead to acts detrimental to the public health and safety is important, the behavioral observation element of fitness-for-duty programs that is required under 10 CFR 26.22(a)(4) also addresses this objective. Therefore, the proposed paragraph would be revised, in part, to eliminate this redundancy.

		In addition, the current provision's requirement for behavioral observation to focus only on detecting behavior changes is too narrow. The NRC intends that behavioral observation must also be conducted in order to increase the likelihood that potentially adverse behavior patterns and actions will be detected and evaluated before there is an opportunity for such behavior patterns or acts to result in detrimental consequences. For example, experience in other industries has shown that an individual's unusual interest in an organization's security activities and operations that are outside the scope of the individual's normal work assignments may be an indication that the individual is gathering intelligence for adversarial purposes. If the behavioral observation element of AA programs focuses only on behavior changes, and an individual has demonstrated a pattern of "unusual interest" since starting work for the licensee, other persons who are aware of the individual's behavior pattern may not consider the behavior to be a potential concern and, therefore, may not raise the concern. As a result, an opportunity to detect and evaluate this behavior pattern would be lost.

		Therefore, in order to increase the effectiveness of the behavioral observation element of AA programs and more clearly convey the NRC's intent, the proposed paragraph would be revised to clarify that the objective of behavioral observation is 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. The portion of current § 73.56(b)(2)(iii) that addresses who must conduct behavioral observation (i.e., supervisors and management personnel) would be moved to a separate paragraph for increased organizational clarity in this section, and would be amended for the reasons discussed with respect to proposed § 73.56(f)(2).
	(f)(1) The licensees, applicants, and C/Vs specified in paragraph (a) of this section shall ensure that the individuals specified in paragraph (b)(1) of this section and, if applicable, (b)(2) of this section are subject to behavioral observation.	Proposed § 73.56(f)(1) would clarify the intent of the current requirement by specifying the individuals who must be subject to behavioral observation. The proposed paragraph would be added to address stakeholder requests at the public meetings discussed in Section IV.3, for increased specificity in the language of the rule.

	(f)(2) The individuals specified in paragraph (b)(1) and, if applicable, (b)(2) of this section shall observe the behavior of other individuals. The licensees, applicants, and C/Vs specified in paragraph (a) of this section shall ensure that individuals who are subject to this section also successfully complete behavioral observation training.	The proposed paragraph would amend the portion of current § 73.56(b)(2)(iii) that requires only supervisors and management personnel to conduct behavioral observation by requiring all individuals who are subject to an authorization program to conduct behavioral observation. Increasing the number of individuals who conduct behavioral observation would enhance the effectiveness of AA programs by increasing the likelihood of detecting behavior or activities that may be adverse to the safe operation and security of the facility and may, therefore, constitute an unreasonable risk to the health and safety and common defense and security. This change is necessary to address the NRC's increased concern with a potential insider threat discussed in Section IV.3. Proposed § 73.56(f)(2) also would require licensees, applicants, and C/Vs to ensure that individuals who are subject to an authorization program successfully complete behavioral observation training. The means by which licensees, applicants, and C/Vs would demonstrate that an individual has successfully completed the training would be through the administration of the comprehensive examination discussed with respect to proposed § 73.56(f)(2)(iii).

		Because all individuals who are subject to the AA program would be required to conduct behavioral observation, training is necessary to ensure that individuals have the knowledge, skills, and abilities necessary to do so.
	(f)(2)(i) Behavioral observation training must be completed before the licensee, applicant, or C/V grants an initial unescorted access authorization, as defined in paragraph (h)(5) of this section, and must be current before the licensee, applicant, or C/V grants an unescorted access authorization update, as defined in paragraph (h)(6) of this section, or an unescorted access authorization reinstatement, as defined in paragraph (h)(7) of this section;	Proposed § 73.56(f)(2)(i) would require all personnel who are subject to this section to complete behavioral observation training before the licensee, applicant, or C/V grants initial unescorted access authorization to the individual, as defined in proposed paragraph (h)(5) [Initial unescorted access authorization]. The proposed rule would also require that an individual's training must be current before the licensee, applicant, or C/V grants an unescorted access authorization update or reinstatement to the individual, as defined in proposed paragraphs (h)(6) [Updated unescorted access authorization] and (h)(7) [Reinstatement of unescorted access authorization reinstatement] of this section, respectively. Annual refresher training, which would be the means by which licensees, applicants, and C/Vs would meet the requirement for training to be "current," would be addressed in proposed § 73.56(f)(2)(ii).

		The proposed requirement to complete behavioral observation training before initial unescorted access authorization is granted is necessary to ensure that individuals have the knowledge, skills, and abilities required to meet their responsibilities for conducting behavioral observation under proposed paragraph (f)(2)(i). The basis for requiring refresher training is discussed with respect to proposed paragraph (f)(2)(ii) of this section.
	(f)(2)(ii) Individuals shall complete refresher training on a nominal 12-month frequency, or more frequently where the need is indicated. Individuals may take and pass a comprehensive examination that meets the requirements of paragraph (f)(2)(iii) of this section in lieu of completing annual refresher training;	Proposed § 73.45(f)(2)(ii) would require annual refresher training in behavioral observation, at a minimum, with more frequent refresher training when the need is indicated. The proposed paragraph would require annual or more frequent refresher training in order to ensure that individuals retain the knowledge, skills, and abilities gained through initial training. Refresher training may also be necessary if an individual demonstrates a failure to implement behavioral observation requirements in accordance with AA program procedures or new information is added to the behavioral observation training curriculum.

		The proposed paragraph would also permit individuals who pass a comprehensive "challenge" examination that demonstrates their continued understanding of behavioral observation to be excused from the refresher training that would otherwise be required under the proposed paragraph. The proposed rule would require that the "challenge" examination must meet the examination requirements specified in proposed paragraph (f)(2)(iii) of this section and individuals who did not pass would undergo remedial training. Permitting individuals to pass a comprehensive "challenge" examination rather than take refresher training each year would ensure that they are retaining their knowledge, skills, and abilities while reducing some costs associated with meeting the annual refresher training requirement.

	(f)(2)(iii) Individuals shall demonstrate the successful completion of behavioral observation training by passing a comprehensive examination that addresses the knowledge and abilities necessary to detect behavior or activities that have the potential to constitute an unreasonable risk to the health and safety of the public and common defense and security, including a potential threat to commit radiological sabotage. Remedial training and re-testing are required for individuals who fail to satisfactorily complete the examination.	Proposed § 73.56(f)(2)(iii) would require individuals to demonstrate that they have successfully completed behavioral observation training by passing a comprehensive examination. The proposed provision would require remedial training and re-testing for individuals who fail to achieve a passing score on the examination. These proposed requirements would be modeled on other required training programs that have been successful in ensuring that examinations are valid and individuals have achieved an adequate understanding of the subject matter.
	(f)(2)(iv) Initial and refresher training may be delivered using a variety of media (including, but not limited to, classroom lectures, required reading, video, or computer-based training systems). The licensee, applicant, or C/V shall monitor the completion of training.	Proposed § 73.56(f)(2)(iv) would permit the use of various media for administering training in order to achieve the efficiencies associated with computer-based training, for example, and other new training delivery technologies that may become available. Permitting the use of various media to administer the training would improve the efficiency of AA programs and reduce regulatory burden, by providing flexibility in the methods that licensees and other entities may use to administer the required training. The proposed paragraph would also require the completion of training to be monitored by the licensee, applicant, or C/V.

		This requirement is necessary to ensure that individuals who are subject to an authorization program actively participate in and receive the required training. The NRC is aware that some individuals have engaged in successful litigation against licensees on the basis that they were not aware of the requirements to which they were subject, in part, because of deficiencies in licensee processes for ensuring that individuals are trained. Therefore, the proposed rule would add this requirement to improve the effectiveness of the training element of AA programs.
	(f)(3) Individuals who are subject to an authorization program under this section shall report to the reviewing official any concerns arising from behavioral observation, including, but not limited to, concerns related to any questionable behavior patterns or activities of others.	Proposed § 73.56(f)(3) would require individuals to report any concerns arising from behavioral observation to the licensee's, applicant's, or C/V's reviewing official. This specificity is necessary because the NRC is aware of past instances in which individuals reported concerns to supervisors or other licensee personnel who did not then inform the reviewing official of the concern. As a result, the concern was not addressed and any implications of the concern for the individual's trustworthiness and reliability were not evaluated.

		Therefore, the proposed rule would require individuals to report directly to the reviewing official, to ensure that the reviewing official is made aware of the concern, has the opportunity to evaluate it, and determine whether to grant, maintain, administratively withdraw, deny, or terminate UAA. The proposed provision would be added to clarify and strengthen the behavioral observation element of AA programs by increasing the likelihood that questionable behaviors or activities are appropriately addressed by the licensees and other entities who are subject to the rule.
	(g) Arrest reporting. Any individual who has applied for or is maintaining unescorted access authorization under this section shall promptly report to the reviewing official any formal action(s) taken by a law enforcement authority or court of law to which the individual has been subject, including an arrest, an indictment, the filing of charges, or a conviction. On the day that the report is received, the reviewing official shall evaluate the circumstances related to the formal action(s) and determine whether to grant, maintain, administratively withdraw, deny, or unfavorably terminate the individual's unescorted access authorization.	A new § 73.56(g) would establish requirements related to the arrest, indictment, filing of charges, or conviction of any individual who is applying for or maintaining UAA under this section. The proposed paragraph would require individuals to promptly report to the reviewing official any such formal action(s) to ensure that the reviewing official has an opportunity to evaluate the implications of the formal action(s) with respect to the individual's trustworthiness and reliability.

		The proposed rule includes other provisions that would also ensure that the reviewing official is aware of and evaluates the implications of any formal action(s) to which an individual may be subject, including the requirement for a criminal history review under proposed § 73.56(d)(7) and regular updates to the criminal history review under proposed § 73.56(i)(1)(v). However, these proposed provisions would not provide for prompt evaluation of any formal action(s) that arise in the intervening time period since a criminal history review was last conducted. Therefore, this requirement would be added to ensure that the reviewing official is made aware of formal actions at the time that they occur, has the opportunity to evaluate the implications of these formal actions with respect to the individual's trustworthiness and reliability, and, if necessary, take timely action to deny or unfavorably terminate the individual's UAA, if the reviewing official determines that the formal actions cast doubt on the individual's trustworthiness and reliability. The proposed rule would also specifically require the formal action(s) to be reported to the licensee's, applicant's, or C/V's reviewing official.

		This specificity is necessary because the NRC is aware of past instances in which individuals reported formal actions to supervisors who did not then inform the reviewing official. As a result, some individuals were granted or maintained UAA without the high assurance that they are trustworthy and reliable that AA programs must provide, as discussed with respect to proposed § 73.56(c) [General performance objective]. Therefore, a specific requirement for individuals to report directly to the reviewing official is necessary to ensure that the reviewing official is aware of the actions, has the opportunity to evaluate the circumstances surrounding the actions, and determine whether to grant, maintain, administratively withdraw, deny, or terminate UAA. The proposed paragraph would not establish a specific time limit within which an individual would be required to report a formal action because the time frames within which different formal actions occur may vary widely, depending on the nature of the formal action and characteristics of the locality in which the formal action is taken. However, nothing in the proposed provision would prohibit licensees, applicants, and C/Vs from establishing, in program procedures, reporting time limits that are appropriate for their local circumstances.

		The proposed rule would use the term, “promptly,” to clarify the NRC’s intent that individuals are responsible for reporting any formal action(s) of the type specified in the proposed paragraph without delay. The proposed paragraph would also require the reviewing official to evaluate the circumstances related to the formal action and decide whether to grant, maintain, administratively withdraw, deny, or unfavorably terminate the individual’s UAA on the day that he or she receives the report of an arrest, indictment, the filing of charges, or conviction. The proposed requirement is necessary because the NRC is aware of past instances in which reviewing officials have been informed of a formal action, but have not acted promptly to evaluate the information and determine its implications with respect to the individual’s trustworthiness and reliability. As a result, some individuals were granted or maintained UAA without the high assurance that they are trustworthy and reliable that AA programs must provide, as discussed with respect to proposed § 73.56(c) [General performance objective].

		The proposed paragraph would provide for the administrative withdrawal of UAA without a positive determination that the individual is trustworthy and reliable (which would permit the granting or maintaining of UAA) or a negative determination of the individual's trustworthiness and reliability (which would require the denial or unfavorable termination of UAA), because the reviewing official may not have sufficient information on the day that the report is received to make the determination. However, if, based on the information available to the reviewing official, he or she is unable to make either a positive or negative determination, the proposed rule would require the administrative withdrawal of UAA until such a determination can be made. The administrative withdrawal of the individual's UAA would be necessary to protect public health and safety and the common defense and security when the trustworthiness and reliability of an individual cannot be positively determined.

§ 73.56(c) *Existing, reinstated, transferred, and temporary access authorization*. (1) Individuals who have had an uninterrupted unescorted access authorization for at least 180 days on April 25, 1991 need not be further evaluated. Such individuals shall be subject to the behavioral observation requirements of this section.	(c)(1) Deleted.	The proposed rule would eliminate current § 73.56(c)(1), which permitted individuals who had an uninterrupted unescorted access authorization for at least 180 days on April 25, 1991, to retain unescorted access authorization and required them to be subject to behavioral observation. The current paragraph would be eliminated because these requirements no longer apply.
§ 73.56(c) *Existing, reinstated, transferred, and temporary access authorization.*	(h) Granting unescorted access authorization. The licensees, applicants, and C/Vs specified in paragraph (a) of this section shall implement the requirements of this paragraph for granting initial unescorted access authorization, updated unescorted access authorization, and reinstatement of unescorted access authorization.	Proposed § 73.56(h) would replace and amend current § 73.56(c), which permits AA programs to specify conditions for reinstating an interrupted UAA, for transferring UAA from another licensee, and for permitting temporary UAA. As discussed in Section IV.3, the requirements in proposed § 73.56 are based upon several fundamental changes to the NRC's approach to access authorization since the terrorist attacks of September 11, 2001, and an increased concern for an active or passive insider who may collude with adversaries to commit radiological sabotage.

		The primary concern, which many of the amendments to § 73.56 are designed to address, is the necessity of increasing the rigor of the access authorization process to provide high assurance that any individual who is granted and maintains UAA is trustworthy and reliable. Proposed § 73.56(h) would identify three categories of proposed requirements for granting UAA: (1) initial unescorted access authorization, (2) updated unescorted access authorization, and (3) reinstatement of unescorted access authorization. The proposed categories, which are based upon whether an individual who has applied for UAA has previously held UAA under § 73.56 and the length of time that has elapsed since the individual's last period of UAA ended, would be defined in proposed § 73.56(h)(5) [Initial unescorted access authorization], proposed § 73.56(h)(6) [Updated unescorted access authorization], and proposed § 73.56(h)(7) [Reinstatement of unescorted access authorization].

		Proposed § 73.56(h) would direct licensees, applicants, and C/Vs to use the criteria for granting UAA that are found in proposed § 73.56(h)(5), (h)(6), and (h)(7), depending on which of the proposed paragraphs would apply to the individual seeking UAA. Current § 73.56 permits authorization programs to specify conditions for reinstating an interrupted UAA or transferring UAA from another licensee, but it does not use the concepts of “initial unescorted access authorization,” “updated unescorted access authorization,” or “reinstatement of unescorted access authorization.” These concepts would be used in proposed § 73.56 to focus the requirements for UAA more precisely on whether the individual has established a “track record” in the industry, and to specify the amount of original information-gathering that licensees, applicants, and C/Vs would be required to perform, based on whether previous AA programs have collected information about the individual.

		For individuals who have established a favorable track record in the industry, the steps that licensees, applicants, and C/Vs would complete in order to grant UAA to an individual would also depend upon the length of time that has elapsed since the individual's last period of UAA was terminated and the amount of supervision to which the individual was subject during the interruption. (The term, ''interruption,'' refers to the interval of time between periods during which an individual maintains UAA under § 73.56 and will be discussed in reference to § 73.56 (h)(4)). In general, the more time that has elapsed since an individual's last period of UAA ended, the more steps that the proposed rule would require licensees, applicants, and C/Vs to complete before granting UAA to the individual. However, if the individual was subject to AA program elements in the recent past, the proposed rule would require licensees, applicants, and C/Vs to complete fewer steps in order to grant UAA to the individual. Individuals who have established a favorable work history in the industry have demonstrated their trustworthiness and reliability from previous periods of UAA, so they pose less potential risk to public health and safety and the common defense and security than individuals who are new to the industry.

		Much is known about these individuals. Not only were they subject to the initial background investigation requirements before they were initially granted UAA, but, while they were working under an AA program, they were watched carefully through ongoing behavioral observation, and demonstrated the ability to consistently comply with the many procedural requirements that are necessary to perform work safely at nuclear power plants. Therefore, the proposed rule would decrease the unnecessary regulatory burden associated with granting UAA under § 73.56 by reducing the steps that AA programs would be required to take in order to grant UAA to such individuals.

	(h)(1) Accepting unescorted access authorization from other authorization programs. Licensees, applicants, and C/Vs who are seeking to grant unescorted access authorization to an individual who is subject to another authorization program that complies with this section may rely on the program elements completed by the transferring authorization program to satisfy the requirements of this section. An individual may maintain his or her unescorted access authorization if he or she continues to be subject to either the receiving licensee's, applicant's, or C/V's authorization program or the transferring licensee's, applicant's, or C/V's authorization program, or a combination of elements from both programs that collectively satisfy the requirements of this section. The receiving authorization program shall ensure that the program elements maintained by the transferring program remain current.	Proposed § 73.56(h)(1) would permit licensees, applicants, and C/Vs to rely upon the authorization programs and program elements of other licensees, applicants or C/Vs, as well as other authorization programs and program elements that meet the requirements of proposed § 73.56, to meet the requirements of this section for granting and maintaining UAA. Proposed § 73.56(h)(1) would update the terminology used in current § 73.56(a)(4), which states that licensees may accept an AA program used by its C/Vs or other organizations provided it meets the requirements of this section. The proposed paragraph would also modify current § 73.56(c)(2), which permits AA programs to specify conditions for transferring UAA from one licensee to another. The proposed paragraph would require the AA program who is receiving an unescorted access authorization that was granted under another AA program to ensure that each of the AA program elements to which individuals must be subject, such as behavioral observation training and psychological re-assessments, remain current, including situations in which the individual is subject to a combination of program elements that are administered separately by the receiving and transferring AA programs.

		The proposed paragraph would increase the specificity of the requirements that must be met by licensees, applicants, or C/Vs for granting UAA and establish detailed minimum standards that all programs must meet. These proposed detailed minimum standards are designed to address recent changes in industry practices that have resulted in a more transient workforce, as discussed in Section IV.3. The authorization programs of licensees, applicants, and C/Vs would be substantially more consistent than in the past under these proposed detailed standards. Therefore, permitting licensees, applicants, and C/Vs to rely on other AA programs to meet the proposed rule's requirements is reasonable and appropriate. In addition, the proposed provisions would reduce unnecessary regulatory burden by eliminating redundancies in the steps required to grant UAA to an individual who is transferring from one program to another.

	(h)(2) Information sharing. To meet the requirements of this section, licensees, applicants, and C/Vs may rely upon the information that other licensees, applicants, and C/Vs who are subject to this section have gathered about individuals who have previously applied for unescorted access authorization and developed about individuals during periods in which the individuals maintained unescorted access authorization.	A new § 73.56(h)(2) would permit licensees and other entities to rely upon information that was gathered by previous licensees, applicants, and C/Vs to meet the requirements of this section. Because information will be shared among licensees, applicants, and C/Vs, this proposed provision would substantially decrease the likelihood that an individual would be inadvertently granted UAA by another licensee after having his or her UAA denied or unfavorably terminated under another program. It also recognizes that there have been changes in staffing practices at power reactors, including a greater reliance on personnel transfers and temporary work forces, as discussed in detail in Section IV.3. For individuals who have previously been evaluated under an authorization program, were granted UAA within the past 3 years, and successfully maintained UAA, this proposed provision would eliminate the need to repeat efforts that were completed as part of the prior access authorization process, thereby saving substantial duplication of effort and expenditure of resources. The proposed provision would work in conjunction with proposed § 73.56(o)(6), which would require a mechanism for information sharing.

		The provision is consistent with the recent access authorization orders and with NRC-endorsed guidance, as well as current industry practices.
	(h)(3) Requirements applicable to all unescorted access authorization categories. Before granting unescorted access authorization to individuals in any category, including individuals whose unescorted access authorization has been interrupted for a period of 30 or fewer days, the licensee, applicant, or C/V shall ensure that —	Proposed § 73.56(h)(3) would establish requirements that the licensee, applicant, or C/V would be required to meet before granting UAA to individuals in any of the categories described in paragraphs (h)(5), (h)(6), or (h)(7) of this section, including individuals whose UAA has been interrupted for a period of 30 or fewer days. The proposed paragraph would clearly specify that the requirements for granting UAA contained in the paragraph are intended to be applied without exceptions to individuals in the specified categories.

	(h)(3)(i) The individual's written consent to conduct a background investigation, if necessary, has been obtained and the individual's true identity has been verified, in accordance with paragraphs (d)(2) and (d)(3) of this section, respectively; (ii) A credit history evaluation or re-evaluation has been completed in accordance with the requirements of paragraphs (d)(5) or (i)(1)(v) of this section, as applicable; (iii) The individual's character and reputation have been ascertained, in accordance with paragraph (d)(6) of this section; (iv) The individual's criminal history record has been obtained and reviewed or updated, in accordance with paragraphs (d)(7) and (i)(1)(v) of this section, as applicable; (v) A psychological assessment or reassessment of the individual has been completed in accordance with the requirements of paragraphs (e) or (i)(1)(v) of this section, as applicable; (vi) The individual has successfully completed the initial or refresher, as applicable, behavioral observation training that is required under paragraph (f) of this section; and	Proposed § 73.46(h)(3)(i) through (h)(3)(vii) would specify the steps required to grant UAA to any individual. The proposed paragraph would require licensees, applicants, and C/Vs to ensure that the individual's written consent for the background investigation in proposed paragraph (h)(3)(i) of this section has been obtained; complete a verification of the individual's true identity in proposed (h)(3)(ii) of this section; ensure completion of the credit history evaluation or re-evaluation, as applicable, in proposed paragraph (h)(3)(ii) of this section; ensure completion of the reference checks required to ascertain the individual's character and reputation in proposed paragraph (h)(3)(iii) of this section; ensure completion of the initial or updated criminal history review, as applicable, in proposed paragraph (h)(3)(iv) of this section; ensure completion of the psychological assessment or re-assessment, as applicable, in proposed paragraph (h)(3)(v) of this section; ensure completion of initial or refresher training in proposed paragraph (h)(3)(vi) of this section; and ensure that the individual has been informed, in writing, or his or her arrest-reporting responsibilities in paragraph (h)(3)(vii) of this section.

	(vii) The individual has been informed, in writing, of his or her arrest-reporting responsibilities under paragraph (g) of this section.	The bases for each of the proposed requirements listed in proposed § 73.56(h)(3)(i) through (h)(3)(vii) are discussed in detail with respect to proposed § 73.56(d)(2), (d)(3), (d)(5) through (d)(7), and (e) through (g), respectively. The bases for the proposed requirements for updates to the credit history evaluation, criminal history review, and psychological assessment are discussed with respect to proposed § 73.56(i)(1)(v). The requirements that authorization programs would be required to meet in order to grant UAA to individuals in every access authorization category would be listed in these paragraphs, in response to stakeholder requests at the public meetings discussed in Section IV.3 for increased clarity in the organizational structure of requirements for granting UAA.

	(h)(4) Interruptions in unescorted access authorization. For individuals who have previously held unescorted access authorization under this section but whose unescorted access authorization has since been terminated under favorable conditions, the licensee, applicant, or C/V shall implement the requirements in this paragraph for initial unescorted access authorization in paragraph (h)(5) of this section, updated unescorted access authorization in paragraph (h)(6) of this section, or reinstatement of unescorted access authorization in paragraph (h)(7) of this section, based upon the total number of days that the individual's unescorted access authorization has been interrupted, to include the day after the individual's last period of unescorted access authorization was terminated and the intervening days until the day upon which the licensee, applicant, or C/V grants unescorted access authorization to the individual. If potentially disqualifying information is disclosed or discovered about an individual, licensees, applicants, and C/Vs shall take additional actions, as specified in the licensee's or applicant's physical security plan, in order to grant or maintain the individual's unescorted access authorization.	Proposed § 73.56(h)(4) would describe the term "interruption," which would be used in proposed § 73.56(h)(5) [Initial unescorted access authorization], proposed § 73.56(h)(6) [Updated unescorted access authorization], and proposed § 73.56(h)(7) and § 73.56(h)(8) [Reinstatement of unescorted access authorization] to refer to the interval of time between periods during which an individual holds UAA under § 73.56. Licensees, applicants, or C/Vs would calculate an interruption in UAA as the total number of days falling between the day upon which the individual's last period of UAA or UA ended and the day upon which the licensee, applicant, or C/V grants UAA to the individual. This change would be made to enhance and clarify the access authorization requirement in current § 73.56(c)(2), which does not define the meaning of the term "interrupted access authorization."

	(h)(5) Initial unescorted access authorization. Before granting unescorted access authorization to an individual who has never held unescorted access authorization under this section or whose unescorted access authorization has been interrupted for a period of 3 years or more and whose last period of unescorted access authorization was terminated under favorable conditions, the licensee, applicant, or C/V shall ensure that an employment history evaluation has been completed in accordance with paragraph (d)(4) of this section. The period of the employment history that the individual shall disclose, and the licensee, applicant, or C/V shall evaluate, must be the past 3 years or since the individual's eighteenth birthday, whichever is shorter. For the 1-year period immediately preceding the date upon which the individual applies for unescorted access authorization, the licensee, applicant, or C/V shall ensure that the employment history evaluation is conducted with every employer, regardless of the length of employment.	A new § 73.56(h)(5) [Initial unescorted access authorization] would establish the category of "initial unescorted access authorization" requirements to apply both to individuals who have not previously held UAA under this section and those whose UAA has been interrupted for a period of 3 or more years and whose last period of UAA ended favorably. In general, the longer the period of time since the individual's last period of UAA ended, the greater the possibility that the individual may have undergone significant changes in lifestyle or character that would diminish his or her trustworthiness and reliability. Therefore, this paragraph would require an individual who has not been subject to an AA program for 3 or more years to undergo the same full and extensive screening to which an individual who has never held UAA would be subject. The proposed paragraph would require the licensee, applicant, or C/V, before granting UAA to an individual, to complete an evaluation of the individual's employment history over the past 3 years. The 3-year time period to be addressed in the employment history evaluation would be consistent with requirements established in the access authorization orders issued by the NRC to nuclear power plant licensees on January 7, 2003, as discussed in Section IV.3.

	For the remaining 2-year period, the licensee, applicant, or C/V 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, if the individual claims employment during the given calendar month.	In addition, this 3-year time period has been used successfully within AA programs since § 73.56 was first promulgated and has met the NRC's goal of ensuring that individuals who are granted UAA are trustworthy and reliable. Therefore, the 3-year time period would be retained in proposed § 73.56. The employment history evaluation would focus on the individual's employment record during the year preceding his or her application for UAA by requiring licensees, applicants, and C/Vs to make a "best effort," as described with respect to proposed § 73.56(d)(4), to obtain and evaluate employment history information from every employer by whom the individual claims to have been employed during the year. The proposed rule would require this focus on the year preceding the individual's application for UAA because the individual's employment history during the past year provides current information related to the individual's trustworthiness and reliability. For the earlier 2 years of the employment history period, the proposed paragraph would require the licensee, applicant, or C/V to conduct the employment history with every employer by whom the applicant claims to have been employed the longest within each calendar month that would fall within that 2-year period.

		The proposed provision would permit this "sampling" approach to the employment history evaluation for the earlier 2-year period because industry experience has shown that employers are often reluctant to disclose adverse information to other private employers about former employees, and that the longer it has been since an individual was employed, the less likely it is that a former employer will disclose useful information. Experience implementing AA programs has also shown that the shorter the time period during which an individual was employed by an employer, the less likely it is that the employer retains any useful information related to the individual's trustworthiness and reliability. Therefore, the proposed paragraph would not require licensees, applicants, and C/Vs to conduct the employment history evaluation with every employer by whom the individual claims to have been employed, but, rather, to contact only the employer by whom the individual claims to have been employed the longest within each calendar month that falls within that 2-year period (i.e., the "given" calendar month). Contacting these employers would increase the likelihood that the employers would have knowledge of the applicant and would be willing to disclose it.

	(h)(6) Updated unescorted access authorization. Before granting unescorted access authorization to an individual whose unescorted access authorization has been interrupted for more than 365 days but fewer than 3 years and whose last period of unescorted access authorization was terminated under favorable conditions, the licensee, applicant, or C/V shall ensure that an employment history evaluation has been completed in accordance with paragraph (d)(4) of this section. The period of the employment history that the individual shall disclose, and the licensee, applicant, or C/V shall evaluate, must be the period since unescorted access authorization was last terminated, up to and including the day the applicant applies for updated unescorted access authorization. For the 1-year period immediately preceding the date upon which the individual applies for unescorted access authorization, the licensee, applicant, or C/V shall ensure that the employment history evaluation is conducted with every employer, regardless of the length of employment.	Proposed § 73.56(h)(6) [Updated unescorted access authorization] would establish a category of "updated unescorted access authorization" to apply to individuals whose UAA has been interrupted for more than 365 days but less than 3 years and whose last period of UAA was terminated favorably. The proposed requirements for granting updated UAA would be less stringent than the proposed requirements for granting initial UAA. The proposed requirements would be less stringent because the individual who is applying for updated UAA would have a more recent "track record" of successful performance within the industry. Also the licensee, applicant, or C/V would have access to information about the individual seeking UAA from the licensee, applicant, or C/V who last granted UAA to the individual as a result of the increased information-sharing requirements of the proposed rule. However, the licensee, applicant, or C/V would not have information about the individual's activities from the period during which the individual's UAA was interrupted. Therefore, the proposed rule's requirements for updated UAA would focus on gathering and evaluating information from the interruption period.

	For the remaining period since unescorted access authorization was last terminated, the licensee, applicant, or C/V 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, if the individual claims employment during the given calendar month.	For example, in the case of an individual whose last period of UAA ended 2 years ago, the licensee, applicant or C/V would gather information about the individual's activities within the 2-year interruption period. Similarly, if an individual's last period of UAA ended 13 months ago, the licensee, applicant, or C/V would gather information about the individual's activities within the past 13 months. For the reasons discussed with respect to proposed § 73.56(h)(5), the proposed paragraph would require the employment history evaluation to be conducted with every employer in the year preceding the individual's application for updated UAA, and to contact only the employer by whom the individual claims to have been employed the longest within any earlier calendar month (i.e., the "given" calendar month) that would fall within the interruption period.

	(h)(7) Reinstatement of unescorted access authorization (31 to 365 days). In order to grant authorization to an individual whose unescorted access authorization has been interrupted for a period of more than 30 days but no more than 365 days and whose last period of unescorted access authorization was terminated under favorable conditions, the licensee, applicant, or C/V shall ensure that an employment history evaluation has been completed in accordance with the requirements of paragraph (d)(4) of this section within 5 business days of reinstating unescorted access authorization. The period of the employment history that the individual shall disclose, and the licensee, applicant, or C/V shall evaluate, must be the period since the individual's unescorted access authorization was terminated, up to and including the day the applicant applies for reinstatement of unescorted access authorization. The licensee, applicant, or C/V 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, if the individual claims employment during a given calendar month.	Proposed § 73.56(h)(7) [Reinstatement of unescorted access authorization] would establish a category of "reinstatement of unescorted access authorization," which would apply to individuals whose UAA has been interrupted for a period of more than 30 days but no more than 365 days and whose last period of UAA was terminated favorably. The proposed steps for reinstating an individual's UAA after an interruption of 365 or fewer days would be less stringent than those required for initial UAA or an updated UAA. This is because these individuals have a recent, positive "track record" within the industry and that record provides evidence that the risk to public health and safety or the common defense and security posed by a less rigorous employment history evaluation is acceptable. The proposed paragraph would limit the period of time to be addressed in the employment history to the period of the interruption in UAA and require that the employment history evaluation must be conducted with the employer by whom the individual claims to have been employed the longest within each calendar month, if the individual claims employment during a given calendar month.

	If the employment history evaluation is not completed within 5 business days due to circumstances that are outside of the licensee's, applicant's, or C/V's control and the licensee, applicant, or C/V is not aware of any potentially disqualifying information regarding the individual within the past 5 years, the licensee, applicant, or C/V may maintain the individual's unescorted access authorization for an additional 5 business days. If the employment history evaluation is not completed within 10 business days of reinstating unescorted access authorization, the licensee, applicant, or C/V may maintain the individual's unescorted access authorization for an additional 5 business days. If the employment history evaluation is not completed within 10 business days of reinstating unescorted access authorization, the licensee, applicant, or C/V shall administratively withdraw the individual's unescorted access authorization until the employment history evaluation is completed.	An employment history for earlier periods of time would be unnecessary because the granting licensee, applicant, or C/V would have access to information about the individual from the licensee, applicant, or C/V who had recently terminated the individual's UAA. However, the licensee, applicant, or C/V would not have information about the individual's activities during the period of interruption, so the proposed rule's requirements for reinstating UAA would focus on gathering and evaluating information only from the interruption period. By contrast to the proposed requirements for an initial UAA and an updated UAA, proposed § 73.56(h)(7) would permit the licensee, applicant, or C/V to reinstate an individual's UAA without first completing the employment history evaluation. As would be required for an updated UAA, the proposed rule would limit the period of time to be addressed by the employment history evaluation to the interruption period.

		However, the proposed paragraph would permit the licensee, applicant, or C/V to reinstate the individual's UAA before completing the employment history evaluation because these individuals have a recent, positive track record within the industry and that record demonstrates that they would pose an acceptable risk to public health and safety or the common defense and security. If the employment history evaluation is not completed within the 5-day period permitted, the proposed paragraph would permit the licensee, applicant, or C/V to maintain the individual's UAA for up to 10 days following the day upon which UAA was reinstated, but only if the licensee, applicant, or C/V is unaware of any potentially disqualifying information about the individual. If the employment history evaluation is not completed within the 10 days permitted, the proposed paragraph would require the licensee, applicant, or C/V to administratively withdraw the individual's UAA until the employment history evaluation is completed. The proposed rule would not establish employment history requirements for individuals whose UAA has been interrupted for 30 or fewer days.

		Proposed § 73.56(h)(3) would require the entities who are subject to this section to obtain and review a personal history disclosure from the applicant for UAA that would address the period since the individual's last period of UAA was terminated. However, the licensee, applicant, or C/V would be permitted to forego conducting an employment history evaluation for individuals whose UAA has been interrupted for such a short period, because there would be little to be learned.
§ 73.56(b)(3) The licensee shall base its decision to grant, deny, revoke, or continue an unescorted access authorization on review and evaluation of all pertinent information developed.	(h)(8) Determination basis. The licensee's, applicant's, or C/V's reviewing official shall determine whether to grant, deny, unfavorably terminate, or maintain or amend an individual's unescorted access authorization status, based on an evaluation of all pertinent information that has been gathered about the individual as a result of any application for unescorted access authorization or developed during or following in any period during which the individual maintained unescorted access authorization.	Proposed § 73.56(h)(8) would amend but retain the meaning of current § 73.56(b)(3), which requires licensees to base a decision to grant, deny, revoke, or continue UAA on review and evaluation of all pertinent information developed. The terms used in the proposed paragraph, such as "unfavorably terminate" to replace "revoke" and "maintain" to replace "continue," would be updated for consistency with the terms currently used by the industry and in other portions of the proposed section. In addition, the proposed paragraph would include references to the reviewing official, rather than the licensee, to convey more accurately that the only individual who is authorized to make access authorization decisions under this section is the designated reviewing official.

	The licensee's, applicant's or C/V's reviewing official may not determine whether to grant unescorted access authorization to an individual or maintain an individual's unescorted access authorization until all of the required information has been provided to the reviewing official and he or she determines that the accumulated information supports a positive finding of trustworthiness and reliability.	The terms, "all pertinent" and "accumulated information," would be used in the proposed paragraph because some of the information that a reviewing official must have before making a determination is gathered under the requirements of 10 CFR Part 26, such as drug and alcohol test results and the results of the suitable inquiry. In addition, the proposed paragraph would expand on the current requirement for a review and evaluation of all pertinent information by adding a prohibition on making an access authorization decision until all of the required information has been provided to the reviewing official and the reviewing official has determined that the information indicates that the subject individual is trustworthy and reliable. These changes would be made to more clearly communicate the NRC's intent by improving the specificity of the language of the rule.

§ 73.56(c)(3) The licensee shall grant unescorted access authorization to all individuals who have been certified by the Nuclear Regulatory Commission as suitable for such access.	(h)(9) Unescorted access for NRC-certified personnel. The licensees and applicants specified in paragraph (a) of this section shall grant unescorted access to all individuals who have been certified by the NRC as suitable for such access including, but not limited to, contractors to the NRC and NRC employees.	Proposed § 73.56(h)(9) would update but retain the meaning of current § 73.56(c)(3), which requires licensees to grant unescorted access to individuals who have been certified by the NRC as suitable for such access. This provision ensures that licensees and applicants are allowed to grant UAA to individuals whom the NRC has determined require such access, and whom the NRC has investigated and is certifying as suitable for access, without requiring the licensees or applicants to meet all of the requirements that would otherwise be necessary before granting unescorted access to these individuals. In addition to avoiding duplication of effort, this proposed provision would help to ensure that NRC-certified individuals will obtain prompt unescorted access to protected and vital areas, if necessary. The proposed paragraph would update the entities who are subject to this requirement by adding applicants to reflect the NRC's new licensing processes for nuclear power plants, as discussed with respect to proposed § 73.56(a).

§ 73.56(b)(4) Failure by an individual to report any previous suspension, revocation, or denial of unescorted access to nuclear power reactors is considered sufficient cause for denial of unescorted access authorization.	(h)(10) Access prohibited. Licensees and applicants may not permit an individual, who is identified as having an access-denied status in the information-sharing mechanism required under paragraph (o)(6) of this section, or has an access authorization status other than favorably terminated, to enter any nuclear power plant protected area or vital area, under escort or otherwise, or take actions by electronic means that could impact the licensee's or applicant's operational safety, security, or emergency response capabilities, under supervision or otherwise, except if, upon review and evaluation, the reviewing official determines that such access is warranted. Licensees and applicants shall develop reinstatement review procedures for assessing individuals who have been in an access-denied status.	A new § 73.56(h)(10) would prohibit the entities who are subject to this section from permitting any individual whose most recent application for UAA has been denied or most recent period of UAA was unfavorably terminated from entering any protected or vital area, or to have the ability to use nuclear power plant digital systems that could adversely impact operational safety, security, or emergency response capabilities. The proposed paragraph would be added because the NRC is aware that, in the past, some licensees permitted individuals whose UAA was denied or unfavorably terminated to enter protected areas as visitors. Licensees' current Physical Security Plans require that any visitor to a protected area or vital area must be escorted and under the supervision of an individual who has UAA and, therefore, is trained in behavioral observation, in accordance with the requirements of this section and related requirements in part 26. However, in the current threat environment, the NRC believes that permitting any individual who has been determined not to be trustworthy and reliable to enter protected or vital areas does not adequately protect public health and safety or the common defense and security. Therefore, the proposed paragraph would prohibit this practice.

		The proposed paragraph would also prohibit individuals whose UAA has been denied or unfavorably terminated from electronically accessing licensees' and applicants' operational safety, security, and emergency response systems. The proposed prohibition on electronic access would be consistent with other requirements in the proposed regulation and is necessary for the same reasons that physical access would be prohibited. An individual whose most recent application for UAA was denied, or whose most recent period of UAA was terminated unfavorably could be considered again for UAA, but only if the applicable requirements are met, as specified in the licensee's or applicant's Physical Security Plan, and the reviewing official makes a positive determination that the individual is trustworthy and reliable, and, therefore, that UAA is warranted. These provisions are necessary to strengthen the effectiveness of AA programs.

	(i) Maintaining access authorization.	A new § 73.56(i) [Maintaining access authorization] would establish the conditions that must be met in order for an individual who has been granted UAA to maintain UAA under this section, and present them together in one paragraph for organizational clarity in the rule. The proposed paragraph would be added in response to stakeholder requests for this clarification at the public meetings discussed in Section IV.3.
	(i)(1) Individuals may maintain unescorted access authorization under the following conditions: (i) The individual remains subject to a behavioral observation program that complies with the requirements of paragraph (f) of this section; (ii) The individual successfully completes behavioral observation refresher training or testing on the nominal 12-month frequency required in (f)(2)(ii) of this section;	Proposed § 73.56(i)(1)(i) and (i)(1)(ii) would reiterate the requirements for subjecting individuals who are maintaining UAA to behavioral observation in proposed paragraph (f) of this section and for successfully completing refresher training or passing a “challenge” examination each year during which the individual maintains UAA in proposed paragraph (f)(2)(ii) of this section. These proposed requirements would be reiterated in this paragraph to emphasize their applicability to maintaining UAA for organizational clarity in the proposed rule. The bases for these proposed requirements are discussed in detail with respect to proposed § 73.56(f) and (f)(2)(ii), respectively.

	(i)(1)(iii) The individual complies with the licensee's, applicant's, or C/V's authorization program policies and procedures to which he or she is subject, including the arrest-reporting responsibility specified in paragraph (g) of this section;	Proposed § 73.56(i)(1)(iii) would require an individual, in order to maintain UAA, to comply with the policies and procedures to which the individual is subject, including the arrest-reporting requirement in proposed paragraph § 73.56(g). The requirement to comply with the applicable licensee's, applicant's, and C/V's policies and procedures would be added because licensees and applicants would establish AA policies and implementing procedures in their Physical Security Plans, required under proposed § 73.56(a), which would include, but would not be limited to, a description of the conditions under which an individual's UAA must be unfavorably terminated. These policies and procedures would prohibit certain acts by individuals, and individuals would be required to avoid committing such acts, in order to maintain UAA. In addition, part 26 requires licensees, applicants, and C/Vs also to develop, implement, and maintain fitness-for-duty program policies and procedures with which individuals must comply in order to maintain UAA. For example, 10 CFR 26.27(b)(3) requires the unfavorable termination of an individual's UAA, if the individual has been involved in the sale, use, or possession of illegal drugs within a nuclear power plant protected area.

		The proposed rule would require compliance with these authorization policies and procedures, as well the arrest-reporting requirement in proposed § 73.56(g), for clarity in the proposed rule. The basis for the arrest-reporting requirement is discussed with respect to proposed § 73.56(g),
	(i)(1)(iv) The individual is subject to a supervisory interview at a nominal 12-month frequency, conducted in accordance with the requirements of the licensee's or applicant's Physical Security Plan; and	Proposed § 73.56(i)(1)(iv) would require individuals, in order to maintain UAA, to be subject to an annual supervisory review during each year that the individual maintains UAA. The supervisory review would be conducted for the purposes and in the manner that licensees and applicants would specify in the Physical Security Plans required under proposed § 73.56(a). The proposed paragraph would include a requirement for these annual supervisory reviews for completeness and organizational clarity in the proposed rule.

	(i)(1)(v) The licensee, applicant, or C/V determines that the individual continues to be trustworthy and reliable. This determination must be made as follows: (A) The licensee, applicant, or C/V shall complete a criminal history update, credit history re-evaluation, and psychological re-assessment of the individual within 5 years of the date on which these elements were last completed, or more frequently, based on job assignment; (B) The reviewing official shall complete an evaluation of the information obtained from the criminal history update, credit history re-evaluation, psychological re-assessment, and the supervisory interview required under paragraph (i)(1)(iv) of this section within 30 calendar days of initiating any one of these elements; (C) The results of the criminal history update, credit history re-evaluation, psychological re-assessment, and the supervisory interview required under paragraph (i)(1)(iv) of this section must support a positive determination of the individual's continued trustworthiness and reliability; and	A new § 73.56(i)(1)(v) would establish requirements for periodic updates of the criminal history review, credit history evaluation, and psychological assessment in order for an individual to maintain UAA. The proposed rule would add these update and re-evaluation requirements because it is necessary to ensure that individuals who are maintaining UAA over long periods of time remain trustworthy and reliable. The proposed update requirements would also apply to transient workers who, under the proposed provisions for granting updated UAA in proposed § 73.56(h)(6) and a reinstatement of UAA in proposed § 73.56(h)(7), may be granted UAA without undergoing the criminal history review, credit history evaluation, and psychological assessment that are required to grant initial UAA in proposed § 73.56(h)(5) each time that the individual transfers between licensee sites or applies for UAA after an interruption period. It is also necessary to ensure that these transient workers remain trustworthy and reliable. Proposed § 73.56(i)(1)(v)(A) would require that the updates and re-evaluation must occur within 5 years of the date on which the program elements were last completed.

	(D) If the criminal history update, credit history re-evaluation, psychological re-assessment, and supervisory review have not been completed and the information evaluated by the reviewing official within 5 years of the initial completion of these elements or the most recent update, re-evaluation, and re-assessment under this paragraph, or within the time period specified in the licensee's or applicant's Physical Security Plans, the licensee, applicant, or C/V shall administratively withdraw the individual's unescorted access authorization until these requirements have been met.	The 5-year interval is consistent with the update requirements of other Federal agencies and private entities who impose similar requirements on individuals who must be trustworthy and reliable. More frequent updates and re-evaluations would be required for some individuals, as specified in the licensee's or applicant's Physical Security Plan, based on the nature of their job assignments, for the reasons discussed with respect to proposed § 73.56(e)(4)(ii). The new § 73.56(i)(1)(v)(B) would also require licensees, applicants, and C/Vs to conduct the required re-evaluation activities that are specified in the proposed paragraph, and the supervisory review required under proposed § 73.56(i)(1)(iv), within 30 days of the initiating any one of these elements. This requirement is necessary to ensure that the reviewing official has the opportunity to review the information collected in the proper context, comparing each element to the other, which would then provide the best possible composite representation of the individual's continued trustworthiness and reliability.

		In a case in which a medical evaluation had been determined to be necessary through the conduct of the psychological re-assessment, the results of the medical evaluation would also become part of the data reviewed by the reviewing official during the 30 day period. Proposed § 73.56(i)(1)(v)(C) would require the reviewing official to determine that the results of the update support a positive determination of the individual's continuing trustworthiness and reliability in order for the individual to maintain UAA. Whereas, § 73.56(i)(1)(v)(D) would require the reviewing official to administratively withdraw the individual's UAA if a positive determination cannot be made, because the information upon which the determination must be made is not yet available. These requirements are necessary to provide high assurance that any individuals who are maintaining UAA have been positively determined to continue to be trustworthy and reliable.

	(i)(2) If an individual who has unescorted access authorization is not subject to an authorization program that meets the requirements of this part for more than 30 continuous days, then the licensee, applicant, or C/V shall terminate the individual's unescorted access authorization and the individual shall meet the requirements in this section, as applicable, to regain unescorted access authorization.	Proposed § 73.56(i)(2) would require licensees, applicants, and C/Vs to terminate an individual's UAA if the individual, for more than 30 [consecutive] days, is not subject to an authorization program that meets the requirements of this section. The requirements of the proposed paragraph would permit an individual to be away from all elements of an AA program for 30 consecutive days in order to accommodate vacations, extended work assignments away from the individual's normal work location, and significant illnesses when the individual would not be reasonably available for behavioral observation. The proposed paragraph would be consistent with industry practices that have been endorsed by the NRC and related requirements in part 26, and added in response to stakeholder requests at the public meetings discussed in Section IV.3.

	(j) Access to vital areas. Each licensee and applicant who is subject to this section shall establish, implement, and maintain a list of individuals who are authorized to have unescorted access to specific nuclear power plant vital areas to assist in limiting access to those vital areas during non-emergency conditions. The list must include only those individuals who require 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.	Proposed § 73.56(j) would amend, and move into § 73.56, current § 73.55(d)(7)(i), which establishes requirements for managing unescorted access to nuclear power plant vital areas. The proposed paragraph would be moved into § 73.56 for organizational clarity in the rule. The proposed requirement is necessary to support the mitigation of the insider threat postulated in 10 CFR 73.1. Specifically, individuals' access to vital areas must be controlled 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 must be terminated. The NRC is aware of many circumstances in the past in which some licensees routinely allowed access to all vital areas for all persons who had been granted unescorted access to a licensee protected area, even during periods when the individuals were not assigned to be working at the licensee site. The defense-in-depth required to mitigate the insider threat requires that even though persons have been determined to be trustworthy and reliable for unescorted access to a protected area and are under behavioral observation, access to vital areas must be restricted to current work-related need.

	(k) Trustworthiness and reliability of background screeners and authorization program personnel. Licensees, applicants, and C/Vs shall ensure that any individuals who collect, process, or have access to personal information that is used to make unescorted access authorization determinations under this section have been determined to be trustworthy and reliable.	A new § 73.56(k) would require licensees, applicants, and C/Vs to ensure that any individuals who collect, process, or have access to the sensitive personal information that is required under this section are, themselves, trustworthy and reliable. The proposed rule would add this provision because the integrity and effectiveness of authorization programs depend, in large part, on the accuracy of the information that is collected about individuals who are applying for or maintaining UAA. Therefore, it is critical that any individuals who collect, process, or have access to the personal information that is used to make UAA determinations are not vulnerable to compromise or influence attempts to falsify or alter the personal information that is collected. Although the NRC is not aware of any instances in which individuals who collected, processed, or had access to personal information were compromised or subject to influence attempts, there have been past circumstances in which it was discovered that persons collecting and reviewing such personal information were found to have extensive criminal histories, which clearly calls into question their trustworthiness and reliability. Therefore, the proposed requirements would be added to strengthen the effectiveness of AA programs.

	(k)(1) Background screeners. Licensees, applicants, and C/Vs 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 authorization determinations shall ensure that a background check of such individuals has been completed and determines that such individuals are trustworthy and reliable. At a minimum, the following checks are required: (i) Verification of the individual's identity; (ii) A local criminal history review and evaluation from the State of the individual's permanent residence; (iii) A credit history review and evaluation; (iv) An employment history review and evaluation for the past 3 years; and (v) An evaluation of character and reputation.	Proposed § 73.56(k)(1) would impose new requirements for determining the trustworthiness and reliability of the employees of any subcontractors or vendors that licensees, applicants, or C/Vs rely upon to collect sensitive personal information for the purposes of determining UAA. The majority of licensees contract (or subcontract, in the case of C/Vs) with other businesses that specialize in background investigation services, typically focused on verifying the employment histories and character and reputation of individuals who have applied for UAA. The proposed paragraph would require that the employees of these firms are themselves trustworthy and reliable, and would establish means by which licensees, applicants, and C/Vs would obtain verification from the subcontractor or vendor that the employees meet the trustworthiness and reliability standards of the licensee, applicant, and C/V.

		Proposed § 73.56(k)(1)(i) through (v) would require a background investigation of these subcontractor or vendor employees to include a verification of the employee's identity, a review and evaluation of the employee's criminal history record from the State in which the employee permanently resides, a credit history review and evaluation, an employment history review and evaluation from the past 3 years, and an evaluation of the employee's character and reputation, respectively. These requirements would be added for the reasons discussed with respect to proposed § 73.56(k).

	(k)(2) Authorization program personnel. Licensees, applicants and C/Vs shall ensure that any individual who evaluates personal information for the purpose of processing applications for unescorted access authorization including, but not limited to a clinical psychologist of psychiatrist who conducts psychological assessments under paragraph (e) of this section; has access to the files, records, and personal information associated with individuals who have applied for unescorted access authorization; or is responsible for managing any databases that contain such files, records, and personal information has been determined to be trustworthy and reliable, as follows: (i) The individual is subject to an authorization program that meets requirements of this section; or (ii) The licensee, applicant, or C/V determines that the individual is trustworthy and reliable based upon an evaluation that meets the requirements of paragraphs (d)(1) through (d)(5) and (e) of this section and a local criminal history review and evaluation from the State of the individual's permanent residence.	A new § 73.56(k)(2) would require that individuals who evaluate and have access to any personal information that is collected for the purposes of this section must be determined to be trustworthy and reliable, and establishes two alternative methods for making this determination. Proposed § 73.56(k)(2)(i) would permit licensees, applicants, and C/Vs to subject such individuals to the process established in this proposed section for granting UAA. Proposed § 73.56(k)(2)(ii) would permit licensees, applicants, or C/Vs to subject such individuals to the requirements for granting UAA in proposed paragraphs (d)(1) through (d)(5) and (e) of this section and a local criminal history review and evaluation from the State of the individuals permanent residence, rather than the criminal history review specified in proposed § 73.56(d)(7). Proposed § 73.56(k)(2)(ii) recognizes that, in some cases, licensees cannot legally obtain the same type of criminal history information about authorization program personnel as they are able to obtain for other individuals who are subject to § 73.56. Therefore, this proposed provision would permit licensees, applicants, and C/Vs to rely on local criminal history checks in such cases. These requirements would be added for the reasons discussed with respect to proposed § 73.56(k).

§ 73.56(e) *Review procedures.* Each licensee implementing an unescorted access authorization program under the provisions of this section shall include a procedure for the review, at the request of the affected employee, of a denial or revocation by the licensee of unescorted access authorization of an employee of the licensee, contractor, or vendor, which adversely affects employment. The procedure must provide that the employee is informed of the grounds for denial or revocation and allow the employee an opportunity to provide additional relevant information, and provide an opportunity for an objective review of the information on which the denial or revocation was based. The procedure may be an impartial and independent internal management review. Unescorted access may not be granted to the individual during the review process.	(l) Review procedures. Each licensee, applicant, and C/V who is implementing an authorization program under this section shall include a procedure for the review, at the request of the affected individual, of a denial or unfavorable termination of unescorted access authorization. The procedure must require that the individual is informed of the grounds for the denial or unfavorable termination and allow the individual an opportunity to provide additional relevant information, and provide an opportunity for an objective review of the information on which the denial or unfavorable termination of unescorted access authorization was based. The procedure may be an impartial and independent internal management review. Licensees and applicants may not grant or permit the individual to maintain unescorted access authorization during the review process.	Proposed § 73.56(l) would retain the meaning of current § 73.56(e) but update some of the terms used in the provision. The proposed paragraph would replace the term, "revocation," with the term, "unfavorable termination," for the reasons discussed with respect to proposed paragraph (d)(1)(iii) of this section. In addition, the proposed paragraph would add references to applicants to reflect the NRC's new licensing processes for nuclear power plants, as discussed with respect to proposed § 73.56(a). Reference to C/Vs would also be added for completeness, as discussed with respected to proposed § 73.56(a)(3).
§ 73.56(f) *Protection of information.* (1) Each licensee, contractor, or vendor who collects personal information on an employee for the purpose of complying with this section shall establish and maintain a system of files and procedures for the protection of the personal information.	(m) Protection of information. Each licensee, applicant, or C/V who is subject to this section who collects personal information about an individual for the purpose of complying with this section shall establish and maintain a system of files and procedures to protect the personal information.	Proposed § 73.56(m) would retain current § 73.56(f)(1) but update it to include reference to applicants and C/Vs for internal consistency in the proposed rule. The current requirement for a system of files and procedures for the protection of information would be moved to proposed §73.56(m)(5) for organizational clarity in the rule.

§ 73.56(f)(2) Licensees, contractors, and vendors small make available such personal information to another licensee, contractor, or vendor provided that the request is accompanied by a signed release from the individual.	(f)(2) Deleted.	Current § 73.56(f)(2) would be deleted, but the intent of the requirement would be incorporated into proposed §73.56(m)(1) for organizational clarity in the rule.

§ 73.56(f)(3) Licensees, contractors, and vendors may not disclose the personal information collected and maintained to persons other than: (ii) NRC representatives; (iii) Appropriate law enforcement officials under court order; (iv) The subject individual or his or her representative; (v) Those licensee representatives who have a need to have access to the information in performing assigned duties, including audits of licensee's, contractor's, and vendor's programs; (vi) Persons deciding matters on review or appeal; or (vii) Other persons pursuant to court order. This section does not authorize the licensee, contractor, or vendor to withhold evidence of criminal conduct from law enforcement officials.	(m)(1) Licensees, applicants, and C/Vs shall obtain a signed consent from the subject individual that authorizes the disclosure of the personal information collected and maintained under this section before disclosing the personal 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 licensees, applicant's or C/V'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 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; and (vii) Other persons pursuant to court order.	Proposed § 73.56(m)(1) would amend current § 73.56(f)(3), which prohibits licensees, applicants, and C/Vs from disclosing personal information collected under this section to any individuals other than those listed in the regulation. The proposed paragraph would continue to permit disclosure of the personal information to the listed individuals, but would add permission for the licensee, applicant, or C/V to disclose the personal information to others if the licensee or other entity has obtained a signed release for such a disclosure from the subject individual. The proposed provision would be added because some licensees have misinterpreted the current requirement as prohibiting them from releasing the personal information under any circumstances, except to the parties listed in the current provision. In some instances, such failures to release information have inappropriately inhibited an individual's ability to obtain information that was necessary for a review or appeal of the licensee's determination for UAA. Therefore, the explicit permission for licensees and other entities to release personal information when an individual consents to the release, in writing, would be to have access to a full and complete evidentiary record in review procedures and legal proceedings.

		Proposed § 73.56(m)(1)(i) through (m)(1)(vii) would list in separate paragraphs the individuals to whom licensees and other entities would be permitted to release personal information about an individual. Proposed § 73.56(m)(1)(ii), (m)(1)(iii), and (m)(1)(vii) would retain the current § 73.56 permission for the release of information to NRC representatives, appropriate law enforcement officials under court order, and other persons pursuant to court order. Proposed § 73.56(m)(1)(i) would retain the current permission for the release of information to the subject individual and his or her designated representative. The proposed paragraph would add requirements for the individual to designate his or her representative in writing and specify the UAA matters to be disclosed. The proposed changes would be made in response to implementation questions from licensees who have sought guidance from the NRC related to the manner in which an individual must “designate” a representative. Proposed § 73.56 (m)(1)(iv) would amend the current reference to licensee representatives who have a need to have access to the information in performing assigned duties. The current rule refers only to individuals who are performing audits of access.

		The intent of the provision was that licensees and C/Vs would be permitted to release information to their representatives who must have access to the personal information in order to perform assigned job duties related to the administration of the program. Therefore, the proposed rule would clarify the provision by adding licensee representatives who perform determinations of trustworthiness and reliability as a further example of individuals who may be permitted access to personal information but only to the extent that such access is required to perform their assigned functions. Proposed § 73.56(m)(1)(v) and (m)(1)(vi) would amend the portion of current § 73.56(f)(3)(vi) that refers to "persons deciding matters on review or appeal." The proposed changes would be made in response to implementation questions from licensees, including whether the rule covers persons deciding matters in judicial proceedings or only the internal review process specified in current § 73.56(e) [Review procedures] as well as whether information could be released in a judicial proceeding that was not initiated by the subject individual. The proposed rule would clarify that the permission includes individuals who are presiding in a judicial or administrative proceeding, but only if the proceeding is initiated by the subject individual.

§ 73.56(f)(3)(i) Other licensees, contractors, or vendors, or their authorized representatives, legitimately seeking the information as required by this section for unescorted access decisions and who have obtained a signed release from the individual.	(m)(2) Personal information that is collected under this section must be disclosed to other licensees, applicants, and C/Vs, or their authorized representatives, who are seeking the information for unescorted access authorization determinations under this section and who have obtained a signed release from the subject individual.	Proposed § 73.56(m)(2) would enhance the current requirement for the disclosure of relevant information to licensees, applicants, and C/Vs, and their authorized representatives who have a legitimate need for the information and a signed release from an individual who is seeking UAA under this part. This proposed provision would be added to further clarify current § 73.56 requirements because some licensees have misinterpreted the current provision as prohibiting the release of information to C/Vs who have licensee-approved authorization programs and require such information in determining individuals' trustworthiness and reliability. The proposed change would be made in order to further clarify the NRC's intent that C/Vs shall have access to personal information for the specified purposes.
	(m)(3) Upon receipt of a written request by the subject individual or his or her designated representative, the licensee, applicant or C/V possessing such records shall promptly provide copies of all records pertaining to a denial or unfavorable termination of the individuals unescorted access authorization.	A new § 73.56(m)(3) would require the licensee, applicant, or C/V possessing the records specified in § 73.56(m) to promptly provide copies of all records pertaining to a denial or unfavorable termination of the individual's UAA to the subject individual or his or her designated representative upon written request. This paragraph would be added to protect individuals' ability to have access to a full and complete evidentiary record in review procedures and legal proceedings.

	(m)(4) A licensee's, applicant's, or C/V's contracts with any individual or organization who collects and maintains personal information that is relevant to an unescorted access authorization determination must require that such records be held in confidence, except as provided in paragraphs (m)(1) through (m)(3) of this section.	Proposed § 73.56(m)(4) would require that a licensee's, applicant's, or C/V's contracts with any individual or organization who collects and maintains personal information that is relevant to a UAA determination must require that such records be maintained in confidence. The paragraph would make an exception for the disclosure of information to the individuals identified in § 73.56(m)(1) through (m)(3). This paragraph would be added to ensure that entities who collect and maintain personal information use and maintain those records with the highest regard for individual privacy.
	(m)(5) Licensees, applicants, and C/Vs who collect and maintain personal information under this section, and any individual or organization who collects and maintains personal information on behalf of a licensee, applicant or C/V, shall establish, implement, and maintain a system and procedures for the secure storage and handling of the personal information collected.	A new § 73.56(m)(5) would require licensees, applicants, and C/Vs, and any individual or organization who collects and maintains personal information on their behalf, to establish, implement, and maintain a system and procedures to ensure that the personal information is secure and cannot be accessed by any unauthorized individuals. The proposed rule would add this specific requirement because the NRC is aware of circumstances in which the personal information of individuals applying for UAA has been removed from a C/V's business location and transported to the personal residences of its employees.

		The proposed provision would prohibit such practices in order to further protect the privacy rights of individuals who are subject to the proposed rule.
§ 73.56(f)(3)(vii) Other persons pursuant to court order. This section does not authorize the licensee, contractor, or vendor to withhold evidence of criminal conduct from law enforcement officials.	(m)(6) This paragraph does not authorize the licensee, applicant, or C/V to withhold evidence of criminal conduct from law enforcement officials.	Proposed § 73.56(m)(5) would retain the meaning of the second sentence of current § 73.56(f)(3)(vii), which states that the protection of information requirements in current § 73.56(f)(3)(vii) do not authorize the licensee to withhold evidence of criminal conduct from law enforcement officers, but renumber the second sentence as a separate paragraph. The first sentence of current § 73.56(f)(3)(vii) permits licensees to release personal information about an individual without his or her written consent under a court order. Therefore, the proposed rule would present the second sentence of current § 73.56(f)(3)(vii) is a separate paragraph to emphasize that the prohibition on withholding personal information from law enforcement officials applies to any information that may be developed under the requirements of this section. This change would be made to improve the clarity of the rule.

§ 73.56(g) *Audits.* § 73.56(g)(2) Each licensee retains responsibility for the effectiveness of any contractor and vendor program it accepts and the implementation of appropriate corrective action.	(n) Audits and corrective action. Each licensee and applicant who is subject to this section shall be responsible for the continuing effectiveness of the authorization program, including authorization program elements that are provided by C/Vs, and the authorization programs of any C/Vs that are accepted by the licensee and applicant. Each licensee, applicant, and C/V who is subject to this section shall ensure that authorization programs and program elements are audited to confirm compliance with the requirements of this section and that comprehensive actions are taken to correct any non-conformance that is identified.	Proposed § 73.56(n) [Audits and corrective action] would rename and amend current § 73.56(g) [Audits]. The phrase, "and corrective action," would be added to the section title to emphasize the NRCs intent that licensees, applicants, and C/Vs must ensure that comprehensive corrective actions are taken in response to any violations of the requirements of this section identified from an audit. The second sentence of proposed § 73.56(n) would re-state the requirement for AA program audits in current § 73.56(g)(1) and add a requirement for comprehensive corrective actions to be taken to any violations identified as a result of the audits. These changes would be made because NRC is aware that some licensees have met the requirements for scheduling audits in current § 73.56(g)(1), but have not acted promptly to resolve violations that were identified. Therefore, the proposed requirements would clarify the NRC's intent that comprehensive corrective actions must be taken in response to audit findings. The first sentence of proposed § 73.56(n) would be added to clarify that licensees and applicants are responsible for the continued effectiveness of their AA programs, as well as those C/V programs or program elements upon which they rely to meet the requirements of this section.

		The proposed sentence would retain the meaning of the last sentence of current § 73.56(g)(2), which states that each licensee retains responsibility for the effectiveness of any contractor and vendor program it accepts and the implementation of appropriate corrective action, but would move it to proposed § 73.56(n) for organizational clarity.
§ 73.56(g)(1) Each licensee shall audit its access authorization program within 12 months of the effective date of implementation of this program and at least every 24 months thereafter to ensure that the requirements of this section are satisfied.	(n)(1) Each licensee, applicant and C/V who is subject to this section shall ensure that their entire authorization program is audited as needed, but no less frequently than nominally every 24 months. Licensees, applicants and C/Vs 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.	Proposed § 73.56(n)(1) would retain the required 24-month audit frequency in current § 73.56(g)(1). Licensees, applicants, and C/Vs would be required to monitor program performance indicators and operating experience, and audit AA program elements more frequently than every 24 months, as needed. In determining the need for more frequent audits, the entities who are subject to this section would consider the frequency, nature, and severity of discovered program deficiencies, personnel or procedural changes, previous audit findings, as well as "lessons learned." The proposed change is intended to promote performance-based rather than compliance-based audit activities and clarify that programs must be audited following a significant change in personnel, procedures, or equipment as soon as reasonably practicable.

		The NRC recognizes that AA programs evolve and new issues and problems continue to arise. A high rate of turnover of AA program personnel in contracted services exacerbates this concern. Licensee audits have identified problems that were associated in some way with personnel changes, such as new personnel not understanding their duties or procedures, the implications of actions that they took or did not take, and changes in processes. The purpose of these focused audits would be to ensure that changes in personnel or procedures do not adversely affect the operation of a particular element within the AA program, or function in question. Accordingly, the proposed audit requirement would ensure that any programmatic problems that may result from significant changes in personnel or procedures would be detected and corrected on a timely basis.

§ 73.56(g)(2) Each licensee who accepts the access authorization program of a contractor or vendor as provided for by paragraph (a)(4) of this section shall have access to records and shall audit contractor or vendor programs every 12 months to ensure that the requirements of this section are satisfied.	(n)(2) Authorization program services that are provided to a licensee, or applicant, by C/V 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 on a nominal 12-month frequency. In addition, any authorization program services that are provided to C/Vs by subcontractor personnel who are off site or are not under the direct daily supervision or observation of the C/V's personnel must be audited on a nominal 12-month frequency.	Proposed § 73.56(n)(2) would add a new requirement specifying that if a licensee or applicant relies upon a C/V program or program element to meet the requirements of this section, and if the C/V personnel providing the AA program service are off site or, if they are on site but not under the direct daily supervision or observation of the personnel of the licensee or applicant, then the licensee or applicant must audit the C/V program or program element on a nominal 12-month frequency. The proposed rule would also require that any authorization program services that are provided to C/Vs by subcontractor personnel who are off site or are not under the direct daily supervision or observation of the C/V's personnel must be audited on a nominal 12-month frequency. The activities of C/V personnel who work on site and are under the daily supervision of AA program personnel would be audited under proposed § 73.56(n). The proposed rule expands and clarifies the current requirement in § 73.56(g)(2), which requires licensees who accept the access authorization program of a contractor or vendor to audit the C/V programs every 12 months, but does not distinguish between C/V personnel who work off site and other C/V personnel, and does not address personnel who work as subcontractors to C/Vs.

		Requiring annual audits for C/V personnel who work off site and for C/V subcontractors is necessary to ensure that the services provided continue to be effective, given that other means of monitoring their effectiveness, such as daily oversight, are unavailable.
	(n)(3) Licensees' and applicants' contracts with C/Vs must reserve the right to audit the C/V and the C/V's subcontractors providing 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.	Proposed § 73.56(n)(3) would add a new requirement that addresses contractual relationships between licensees, applicants, and C/Vs. The proposed rule would specify that contracts between licensees, applicants, and C/Vs must allow the licensees or applicants the right to audit the C/Vs and the C/V's subcontractors providing 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 AA program. The proposed paragraph would apply to any C/V with whom the licensee or applicant contracts for authorization program services. The proposed rule would specify that contracts must allow audits at unannounced times, which the NRC considers necessary to enhance the effectiveness of the audits.

		Such unannounced audits could be necessary, for example, if a licensee or applicant receives an allegation that an off-site C/V is falsifying records and the licensee or applicant determines that an unannounced audit would provide the most effective means to investigate such an allegation. The proposed paragraph would ensure that the licensee's or other entity's contract with the C/V would permit the unannounced audit as well as access to any information necessary to conduct the audit and ensure the proper performance of the AA program.
	(n)(4) Licensees' and applicants' contracts with C/Vs, and a C/V's contracts with subcontractors, must also require that the licensee or applicant shall be provided with, or permitted access to, copies of any documents and take away any documents, that may be needed to assure that the C/V and its subcontractors are performing their functions properly and that staff and procedures meet applicable requirements.	A new § 73.56(n)(4) would ensure that licensees' and applicants' contracts with C/Vs permit the licensee or applicant to be provided with or permitted to obtain copies of and take away any documents that auditors may need to assure that the C/V or its subcontractors are performing their functions properly and that staff and procedures meet applicable requirements. This proposed provision would respond to several incidents in which parties under contract to licensees did not permit AA program auditors to remove documents from a C/V's premises that were necessary to document audit findings, develop corrective actions, and ensure that the corrective actions were comprehensive and effective.

	(n)(5) Audits must focus on the effectiveness of the authorization program or program element(s), as appropriate. At least one member of the audit team shall be a person who is knowledgeable of and practiced with meeting authorization program performance objectives and requirements. The individuals performing the audit of the authorization program or program element(s) shall be independent from both the subject authorization programs management and from personnel who are directly responsible for implementing the authorization program(s) being audited.	A new § 73.56(n)(5) would require audits to focus on the effectiveness of AA programs and program elements in response to industry and NRC experience that some licensees' AA program audits have focused only on the extent to which the program or program elements meet the minimum regulatory requirements in the current rule. Consistent with a performance-based approach, the proposed paragraph would more clearly communicate the NRC's intent that AA programs must meet the performance objective of providing high assurance that individuals who are subject to the program are trustworthy and reliable, and do not constitute an unreasonable risk to public health and safety or the common defense and security, including the potential to commit radiological sabotage. The proposed paragraph would also require that the audit team must include at least one individual who has practical experience in implementing all facets of AA programs and that the team members must be independent. These provisions would be added in response to issues that have arisen since the requirements for AA programs were first promulgated, in which licensee audits were ineffective because the personnel who conducted the audits:

		(1) lacked the requisite knowledge to evaluate the wholistic implications of individual requirements or the complexities associated with meeting the rule's performance objective and, therefore, could not adequately evaluate program effectiveness, or (2) were not independent from the day-to-day operation of the AA program and, therefore, could not be objective, because in some cases, these persons were auditing their own activities. The proposed requirements would be necessary to correct these audit deficiencies.
	(n)(6) The result of the audits, along with any recommendations, must be documented and reported to senior corporate and site management. Each audit report must identify conditions that are adverse to the proper performance of the authorization program, the cause of the condition(s), and, when appropriate, recommended corrective actions, and corrective actions taken. The licensee, applicant or C/V shall review the audit findings and take any additional corrective actions, to include re-auditing of the deficient areas where indicated, to preclude, within reason, repetition of the condition. The resolution of the audit findings and corrective actions must be documented.	Proposed § 73.56(n)(6) would clarify the requirements for documentation and dissemination of audit results. Section 73.56(h)(2) of the current rule specifies that licensees shall retain records of results of audits, resolution of the audit findings, and corrective actions. The proposed rule would retain the requirement that licensees, applicants, and C/Vs document audit findings. The proposed rule would add a requirement that any recommendations must be documented, and also would add a requirement that findings and recommendations must be reported to senior corporate and site management. The proposed rule specifies more fully than the current rule what an audit report must contain.

		The second sentence of the proposed paragraph would require each audit report to identify conditions that are adverse to the proper performance of the AA program, the cause of the condition(s), and, when appropriate, recommended corrective actions, and corrective actions already taken. The third sentence of the proposed paragraph would require the licensee, applicant, or C/V to review the audit findings and, where warranted, take additional corrective actions, to include re-auditing of the deficient areas where indicated, to preclude, within reason, repetition of the condition. Finally, the proposed rule would require the resolution of the audit findings and corrective actions to be documented. The current rule does not state explicitly that resolution of the audit findings and corrective actions must be documented; it provides only that records of resolution of the audit findings and corrective actions must be retained for 3 years. The additional sentences in the proposed rule would provide consistency with Criterion XVI in appendix B to 10 CFR Part 50 and would indicate that AA audit reports must be included in licensees' and applicants' corrective action programs, and that any nonconformance is not only identified, but corrected.

	(n)(7) Licensees and applicants may jointly conduct audits, or may accept audits of C/Vs that were conducted by other licensees and applicants who are subject to this section, if the audit addresses the services obtained from the C/V by each of the sharing licensees and applicants. C/Vs may jointly conduct audits, or may accept audits of its subcontractors that were conducted by other licensees, applicants and C/Vs who are subject to this section, if the audit addresses the services obtained from the subcontractor by each of the sharing licensees, applicants and C/Vs.	Proposed § 73.56(n)(7) would clarify the circumstances in which licensees, applicants, and C/Vs may accept and rely on others' audits. The current rule in § 73.56(g) states only that licensees may accept audits of contractors and vendors conducted by other licensees. The proposed rule would amend the current provision to incorporate specific permission for licensees and other entities to jointly conduct audits as well as rely on one anothers audits, if the audits upon which they are relying address the services obtained from the C/V by each of the sharing licensees or applicants. These proposed changes would make the rule consistent with current licensee practices that have been endorsed by the NRC and reduce unnecessary regulatory burden by reducing the number of redundant audits that would be performed.

	(n)(7)(i) Licensees, applicants and C/Vs 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 C/V relies are audited, if the program elements and services were not addressed in the shared audit.	Proposed § 73.56(n)(7)(i) would require licensees, applicants, and C/Vs to identify any areas that were not covered by a shared or accepted audit and ensure that any unique services used by the licensee, applicant, or C/V that were not covered by the shared audit are audited. The proposed provision is necessary to ensure that all authorization program elements and services upon which each of the licensees, applicants, and C/Vs relies are audited, and that elements not included in the shared audits are not overlooked or ignored.
§ 73.56(g)(2) ... Licensees may accept audits of contractors and vendors conducted by other licensees.	(n)(7)(ii) Sharing licensees and applicants need not re-audit the same C/V for the same period of time. Sharing C/Vs need not re-audit the same subcontractor for the same period of time.	Proposed § 73.56 (n)(7)(ii) would add a new paragraph clarifying that licensees, applicants, and C/Vs need not re-audit the same C/V for the same period of time, and that C/Vs who share the services of the same subcontractor with other C/Vs or licensees and applicants, need not re-audit the same subcontractor for the same period of time.

		The proposed rule would include this provision in response to implementation questions from stakeholders at the public meetings discussed in Section IV.3 who reported that some industry auditors and quality assurance personnel have misunderstood the intent of the current provision and have required licensees to re-audit C/V programs that have been audited by other licensees during the same time period. However, such re-auditing would be unnecessary, as the shared program elements and services should be identical, and the period of time covered by the audit should be the same nominal 12-month period. Therefore, the proposed provision would be added to clarify the intent of current § 73.56(g)(2).
§ 73.56(g)(2) ... Each sharing utility shall maintain a copy of the audit report, to include findings, recommendations and corrective actions.	(n)(7)(iii) Each sharing licensee, applicant and C/V shall maintain a copy of the shared audit, including findings, recommendations, and corrective actions.	Proposed § 73.56(n)(7)(iii) would retain the requirement in current § 73.56(g)(2) that each sharing entity shall maintain a copy of the shared audit report. The proposed provision would specify that the requirement to retain a copy of a shared audit report includes a requirement to retain a copy of findings, recommendations, and corrective actions, and that the requirement pertains to each sharing licensee, applicant and C/V. This provision is necessary to ensure that the audit documents are available for NRC review.

§ 73.56(h) *Records.* § 73.56(h)(1) Each licensee who issues an individual unescorted access authorization shall retain the records on which the authorization is based for the duration of the unescorted access authorization and for a five-year period following its termination.	(o) Records. Each licensee, applicant, and C/V who is subject to this section 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.	Proposed § 73.56(o) [Records] would establish a requirement that licensees, applicants and C/Vs who are subject to this section must retain the records required under the proposed rule for either the periods that are specified by the appropriate regulation or for the life of the facility's license, certificate, or other regulatory approval, if no records retention requirement is specified. The proposed rule would replace the current records requirement in § 73.56(h)(1), which requires retention of records on which UAA is granted for a period of 5 years following termination of UAA, and retention of records upon which a denial of UAA is based for 5 years, and in § 73.56(h)(2), which requires retention of audit records for 3 years. The proposed records retention requirement is a standard administrative provision that is used in all other parts of 10 CFR that contain substantive requirements applicable to licensees and applicants.

	(o)(1) All 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.	Proposed § 73.56(o)(1) would permit the records that would be required under the provisions of the proposed section to be stored and archived electronically if the method used to create the electronic records: (1) provides an accurate representation of the original records; (2) prevents access to the information by any individuals who are not authorized to have such access; (3) prevents the alteration of any archived information and/or data once it has been committed to storage; and (4) allows easy retrieval and re-creation of the original records. The proposed paragraph would be added to recognize that most records are now stored electronically and must be protected to ensure the integrity of the data. Records are now stored electronically and must be protected to ensure the integrity of the data.

	(o)(2) Each licensee, applicant, and C/V who is subject to this section shall retain the following records for at least 5 years after the licensee, applicant, or C/V terminates or denies an individual's unescorted access authorization or until the completion of all related legal proceedings, whichever is later: (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 authorization; (ii) Records pertaining to denial or unfavorable termination of unescorted access authorization and related management actions; and (iii) Documentation of the granting and termination of unescorted access authorization.	Proposed § 73.56(o)(2) would require licensees, applicants, and C/Vs to retain certain records related to UAA determinations for at least 5 years after an individual's UAA has been terminated or denied, or until the completion of all related legal proceedings, whichever is later. The proposed requirement to retain records until the completion of all related legal proceedings would address the fact that legal actions involving records of the type specified in the proposed paragraph can continue longer than the 5 years that the current rule requires these records to be retained. Adding a requirement to retain the records until all legal proceedings are complete would protect individuals' ability to have access to a full and complete evidentiary record in legal proceedings. The proposed rule would identify more specifically the records to be retained than the current rule, which in § 73.56(h)(1) specifies only "the records on which authorization is based" and "the records on which denial is based." Proposed § 73.56(o)(2) would require licensees, applicants, and C/Vs to retain three specified types of records:

		(1) Records listed in proposed § 73.56(o)(2)(i), which specifies records of the information that must be collected under § 73.56(d) [Background investigation] and § 73.56(e) [Psychological assessment] of the proposed rule that results in the granting of UAA; (2) records listed in proposed § 73.56(o)(2)(ii), which specifies records pertaining to denial or unfavorable termination of UAA and related management actions; and (3) records listed in proposed § 73.56(o)(2)(iii), which specifies documentation of the granting and termination of UAA. Proposed § 73.56(o)(2)(iii), requiring retention of records that are related to the granting and termination of an individual's UAA, would be added to ensure that licensees, applicants, and C/Vs who may be considering granting UAA to an individual can determine which category of UAA requirements would apply to the individual, based upon the length of time that has elapsed since the individual's last period of UAA was terminated and whether the individual's last period of UAA was terminated favorably.

§ 73.56(h)(2) Each licensee shall retain records of results of audits, resolution of the audit findings and corrective actions for three years.	(o)(3) Each licensee, applicant, and C/V who is subject to this section shall retain the following records for at least 3 years or until the completion of all related legal 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.	Proposed § 73.56(o)(3)(i) and (ii) would require licensees, applicants, and C/Vs to retain records related to behavioral observation training and records related to audits, audit findings, and corrective actions for at least 3 years, or until the completion of all related legal proceedings, whichever is later. Proposed § 73.56(o)(3)(i) would add a new requirement, not addressed in the current rule, to retain records of behavioral observation training. Because the proposed rule is adding a requirement that all individuals who are subject to the AA program must perform behavioral observation, and therefore that they must all be trained in behavioral observation, this proposed record retention requirement is necessary to allow the NRC to review the implementation of the training requirement. Proposed § 73.56(o)(3)(i) would retain the 3-year recordkeeping requirements of the current rule in § 73.56(h)(2) for audit findings and corrective action records.

	(o)(4) Licensees, applicants, and C/Vs shall retain written agreements for the provision of services under this section for the life of the agreement or until completion of all legal proceedings related to a denial or unfavorable termination of unescorted access authorization that involved those services, whichever is later.	Proposed § 73.56(o)(4) would add a new requirement that licensees, applicants, and C/Vs shall retain written agreements for the provision of authorization program services for the life of the agreement or until completion of all legal proceedings related to a denial or unfavorable termination of UAA that involved those services, whichever is later. The proposed requirement for retention of the agreement for the life of the agreement would ensure that the agreement is available for use as a source of information about the scope of duties under the agreement. The proposed requirement to retain the written agreements for any matter under legal challenge until the matter is resolved is necessary to ensure that the materials remain available, should an individual, the NRC, a licensee, or another entity who would be subject to the rule require access to them in a legal or regulatory proceeding.

	(o)(5) Licensees, applicants, and C/Vs shall retain records of the background checks, and psychological assessments of 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 C/V, or until the completion of any legal proceedings relating to the actions of such authorization program personnel, whichever is later.	Proposed § 73.56(o)(5) would be added to require licensees, applicants, and C/Vs to retain records related to the background checks and psychological assessments of AA program personnel, conducted under proposed paragraphs (d) and (e) of § 73.56, for the length of the individual's employment by or contractual relationship with the licensee, applicant, or C/V, or until the completion of all related legal proceedings, whichever is later. The proposed period during which these records must be maintained would be based on the NRC's need to have access to the records for inspection purposes and the potential need for the records to remain available should an individual, the NRC, a licensee, or another entity who would be subject to this rule require access to them in a legal or regulatory proceeding. However, the proposed rule would establish a limit on the period during which the records must be retained in order to reduce the burden associated with storing such records indefinitely.

	(o)(6) Licensees, applicants, and C/Vs shall ensure that the information about individuals who have applied for unescorted access authorization, which is specified in the licensee's or applicant's Physical Security Plan, is recorded and retained in an information-sharing mechanism that is established and administered by the licensees, applicants, and C/Vs who are subject to his section. Licensees, applicants, and C/Vs shall ensure that only correct and complete information is included in the information-sharing mechanism. If, for any reason, the shared information used for determining an individual's trustworthiness and reliability changes or new information is developed about the individual, licensees, applicants, and C/Vs shall correct or augment the shared information contained in the information-sharing mechanism.	A new § 73.56(o)(6) would require licensees, applicants and C/Vs to establish and administer an information-sharing mechanism (i.e., a database) that permits all of the entities who are subject to §73.56 to access certain information about individuals who have applied for UAA under this section. The information that must be shared would be specified in the Physical Security Plans that licensees and entities would be required to submit for NRC review and approval under proposed §73.56(a). The proposed paragraph would require licensees, applicants, and C/Vs to enter this information about individuals who have applied for UAA into the information-sharing mechanism and update the shared information, if the licensee, applicant or C/V determines that information previously entered is incorrect or develops new information about the individual. The proposed requirement for an information-sharing mechanism is necessary to address several long-standing weaknesses in the sharing of information about individuals among licensee and C/V authorization programs that is required under current §73.56.

	If the changed or developed information has implications for adversely affecting an individual's trustworthiness and reliability, the licensee, applicant, or C/V who has discovered the incorrect information, or develops new information, shall inform the reviewing official of any authorization program under which the individual is maintaining unescorted access authorization of the updated information on the day of discovery. The reviewing official shall evaluate the information and take appropriate actions, which may include denial or unfavorable termination of the individual's unescorted access authorization. If, for any reason, the information-sharing mechanism is unavailable and a notification of changes or updated information is required, licensees, applicants, and C/Vs shall take manual actions to ensure that the information is shared, and update the records in the information-sharing mechanism as soon as reasonably possible. Records maintained in the database must be available for NRC review.	Although the industry has maintained a database for many years, some licensees did not participate, some programs did not enter complete information, some programs did not enter the information in a timely manner, and C/Vs who were implementing authorization programs were not permitted to participate. As a result, some licensees and C/Vs were at risk of granting UAA to individuals without being aware, in a few instances, that the individual's last period of UAA had been terminated unfavorably or that potentially disqualifying information about the individual had been developed by a previous licensee after the individual was granted UAA by a subsequent licensee, because that additional information was not communicated. Therefore, the proposed rule would require establishing and administering an information-sharing mechanism to strengthen the effectiveness of authorization programs by ensuring that information that has implications for an individual's trustworthiness and reliability is available in a timely manner, accurate, and complete.

		The proposed paragraph would also require licensees, applicants, and C/Vs to inform the reviewing official of any licensee, applicant, or C/V who may be considering an individual for UAA or has granted UAA to an individual of any corrected or new information about that individual on the day that incorrect or new information is discovered. The proposed requirement to inform the subsequent licensee's, applicant's, or C/V's reviewing official would be added to ensure that the corrected or new information is actively communicated, in addition to entering it into the information-sharing mechanism. The proposed rule would also require the receiving reviewing official to evaluate the corrected or new information and determine its implications for the individual's trustworthiness and reliability. If the information indicates that the individual cannot be determined to be trustworthy and reliable, the proposed rule would require the receiving reviewing official to deny or unfavorably terminate the individual's UAA.

		The proposed requirement to inform subsequent AA programs of corrected or new information is necessary because receiving AA programs would not otherwise become aware of the information unless and until the individual seeks UAA from another AA program or is subject to the re-evaluation required under proposed § 73.56(i)(1)(v). The proposed paragraph would also require licensees, applicants, and C/Vs to take manual actions to share the required information, if the industry database is unavailable for any reason. These manual actions could include, but would not be limited to, telephone contacts, faxes, and email communications. However, the proposed rule would also require that any records created manually must be entered into the database once it is again available. These provisions would be necessary to maintain the effectiveness of the information-sharing component of AA programs. Finally, the proposed paragraph would also require the information-sharing mechanism to be available for NRC review. This requirement is necessary to ensure that NRC personnel have access to the information-sharing mechanism for required inspection activities.

	(o)(7) If a licensee, applicant, or C/V administratively withdraws an individual's unescorted access authorization under the requirements of this section, the licensee, applicant, or C/V may not record the administrative action to withdraw the individual's unescorted access authorization as an unfavorable termination and may not disclose it in response to a suitable inquiry conducted under the provisions of part 26 of this chapter, a background investigation conducted under the provisions of this section, or any other inquiry or investigation. Immediately upon favorable completion of the background investigation element that caused the administrative withdrawal, the licensee, applicant, or C/V shall ensure that any matter that could link the individual to the temporary 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 the individual's unescorted access.	A new § 73.56(o)(7) would ensure that the temporary administrative withdrawal of an individual's UAA, caused by a delay in completing any portion of the background investigation or re-evaluation that is not under the individual's control, would not be treated as an unfavorable termination, except if the reviewing official determines that the delayed information requires denial or unfavorable termination of the individual's UAA. This proposed provision would be necessary to ensure that individuals are not unfairly subject to any adverse consequences for the licensee's or other entity's delay in completing the background investigation or other requirements of the proposed section.

Table 4 - Proposed Part 73; § 73.58
Safety/security interface.

PROPOSED LANGUAGE	CONSIDERATIONS
§73.58 Safety/security interface requirements for nuclear power reactors.	Proposed § 73.58 would be a new requirement in part 73. The need for the proposed rulemaking is based on: (i) the Commission's comprehensive review of its safeguards and security programs and requirements, (ii) the variables in the current threat environment, (iii) the analyses made during the development of the changes to the Design Basis Threat, (iv) the plant-specific security analyses, and (v) the increased complexity of licensee security measures now being required with an attendant increase in the potential for adverse interactions between safety and security. Additionally, it is based on plant events 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 Commission has determined that the proposed safety/security rule requirements are necessary for reasonable assurance that the public health and safety and common defense and security continue to be adequately protected because the current regulations do not specifically require evaluation of the effects of plant changes on security or the effects of security plan changes on plant safety. Further, the regulations do not require communication about the implementation and timing of changes, which would promote awareness of the effects of changing conditions, and result in appropriate assessment and response.

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. (a)(1) The licensee shall assess and manage the potential for adverse affects on safety and security, including the site emergency plan, before implementing changes to plant configurations, facility conditions, or security.	The introductory text would indicate this section would apply to power reactors licensed under 10 CFR Parts 50 or 52. Paragraph (a)(1) of this section would require 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 would be identified, the licensee shall take appropriate measures to manage the potential adverse effect. Managing the potential adverse effect would be further described in paragraph (b). The requirements of the proposed § 73.58 would be additional requirements to assess proposed changes and to manage potential adverse effects contained in other NRC regulations, and would not be intended to substitute for them. The primary function of this proposed rule would be 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 (a)(1) would not be required so as not to delay plant and security actions unnecessarily.
(a)(2) 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).	Paragraph (a)(2) of this section would identify that changes identified by either planned or emergent activities must be assessed by the licensee. Paragraph (a)(2) of this section would also provide a description of typical activities for which changes must be assessed and for which resultant adverse interactions must be managed.

(b) 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.	Paragraph (b) of this section would require that, when potential adverse interactions would be identified, licensees shall communicate the potential adverse interactions to appropriate licensee personnel. The licensee shall also take appropriate compensatory and mitigative actions to maintain safety and security consistent with the applicable NRC requirements. The compensatory and/or mitigative actions taken must be consistent with existing requirements for the affected activity.

Table 5 - Proposed Part 73; § 73.71

Reporting of safeguards events

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
	(a) Each licensee subject to the provisions of § 73.55 shall notify the NRC Operations Center,[1] as soon as possible but not later than 15 minutes after discovery of an imminent or actual safeguards threat against the facility and other safeguards events described in paragraph I of appendix G to this part.[2] Footnote: 1. Commercial (secure and non-secure) telephone number of the NRC Operations Center are specified in appendix A to this part. Footnote: 2. Notifications to the NRC for the declaration of an emergency class shall be performed in accordance with § 50.72 of this chapter.	This paragraph would be added to provide for the very rapid communication to the Commission of an imminent or actual threat to a power reactor facility. The proposed 15-minute requirement would more accurately reflect the current threat environment. Because an actual or imminent threat could quickly result in a security event, a shorter reporting time would be required. This shortened time would permit the NRC to contact Federal authorities and other licensees in a rapid manner to inform them of this event, especially if this event is the opening action on a coordinated multiple-target attack. Such notice may permit other licensees to escalate to a higher protective level in advance of an attack. The Commission would expect licensees to notify the NRC Operations Center as soon as possible after they notify local law enforcement agencies, but within 15 minutes. The Commission may consider the applicability of this requirement to other types of licensees in future rulemaking.

Table 5 - Proposed Part 73; § 73.71

Reporting of safeguards events

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
		Footnote 1 would provide a cross reference to appendix A to part 73 which contains NRC contact information. Footnote 2 would remind licensees of their concurrent emergency declaration responsibilities under 10 CFR 50.72.
	(a)(1) When making a report under paragraph (a) of this section, the licensees shall:	The proposed rule would include this introductory statement, which provides a structure for the following list of information to be provided in the 15-minute report.
	(a)(1)(i) Identify the facility name; and	This requirement would be added to ensure the licensee's facility is clearly identified when a report is made.
	(a)(1)(ii) Briefly describe the nature of the threat or event, including:	This requirement would be added to ensure the nature and substance of the event would be clearly articulated based on the best information available to the licensee at the time of the report. The information should be as factual and as succinct as possible. Additional information regarding the identification of events to be reported and the nature of the information to be provide will be described in guidance.

Table 5 - Proposed Part 73; § 73.71

Reporting of safeguards events

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
	(a)(1)(ii)(A) Type of threat or event (e.g., armed assault, vehicle bomb, credible bomb threat, etc.); and	This requirement would be added to provide for a minimum, succinct categorization of the information described in the report. This would allow the licensee the opportunity provide a scope for the information included in the report. The information should be as factual and as succinct as possible at the time of the report. Additional information regarding identification of events to be reported will be provided in guidance.
	(a)(1)(ii)(B) Threat or event status (i.e., imminent, in progress, or neutralized)	This requirement would be added to provide information regarding the most current status of the event or information being reported. The information should be as factual as possible at the time of the report.
(b)(2) This notification must be made in accordance with the requirements of Paragraphs (a) (2), (3), (4), and (5) of this section.	(a)(2) Notifications must be made according to paragraph (e) of this section, as applicable.	This paragraph would be revised to reflect the new location for the methods for these notifications. The requirements for the methods all of the verbal notifications [under this section] would be consolidated under paragraph (e).

Table 5 - Proposed Part 73; § 73.71

Reporting of safeguards events

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
(a) (1) Each licensee subject to the provisions of §§73.25, 73.26, 73.27(c), 73.37, 73.67(e), or 73.67(g) shall notify the NRC Operations Center[1] within one hour after discovery of the loss of any shipment of SNM or spent fuel, and within one hour after recovery of or accounting for such lost shipment. Footnote: 1. Commercial telephone number of the NRC Operation Center is (301) 816-5100.	(b) Each licensee subject to the provisions of §§ 73.25, 73.26, 73.27(c), 73.37, 73.67(e), or 73.67(g) shall notify the NRC Operations Center within one (1) hour after discovery of the loss of any shipment of special nuclear material (SNM) or spent nuclear fuel, and within one (1) hour after recovery of or accounting for the lost shipment. Notifications must be made according to paragraph (e) of this section, as applicable.	This requirement would be renumbered and retained with minor revision. Footnote (1) would be relocated to new paragraph (a) and revised. The acronym "SNM" would be spelled out as "special nuclear material." The word "nuclear" would be added to "spent fuel" to be consistent with terminology used elsewhere in Part 73. Reference to the methods of telephonic reporting would be added to specify paragraph (e) of this section.
(b)(1) Each licensee subject to the provisions of §§73.20, 73.37, 73.50, 73.51, 73.55, 73.60, or 73.67 shall notify the NRC Operations Center within 1 hour of discovery of the safeguards events described in Paragraph I(a)(1) of appendix G to this part.	(c) Each licensee subject to the provisions of §§ 73.20, 73.37, 73.50, 73.51, 73.55, 73.60, or 73.67 shall notify the NRC Operations Center within one (1) hour after discovery of the safeguards events described in paragraph II of appendix G to this part. Notifications must be made according to paragraph (e) of this section, as applicable.	This requirement would be renumbered and retained with minor revision. The words "1 hour of" would be replaced by the words "one (1) hour after" to clarify the time frame established by this requirement. The reference to appendix G would be revised as a conforming change to specify the events to be reported. Reference to the methods of reporting would be added to specify paragraph (e) of this section.

Table 5 - Proposed Part 73; § 73.71

Reporting of safeguards events

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
	(d) Each licensee subject to the provisions of § 73.55 shall notify the NRC Operations Center, as soon as possible but not later than four (4) hours after discovery of the safeguards events described in paragraph III of appendix G to this part. Notifications must be made according to paragraph (e) of this section, as applicable.	This paragraph would be added to provide a requirement for power reactor licensees to notify the Commission of suspicious activities, attempts at access, etc., that may indicate pre-operational surveillance, reconnaissance, or intelligence gathering activities targeted against the facility. This would more accurately reflect the current threat environment; would assist the Commission in evaluating threats to multiple licensees; and would assist the intelligence and homeland security communities in evaluating threats across critical infrastructure sectors. The reporting process intended in this proposed rule would be similar reporting process that the licensees currently use under guidance issued by the Commission subsequent to September 11, 2001, and would formalize Commission expectations; however, the reporting interval would be lengthened from 1 hour to 4 hours.

Table 5 - Proposed Part 73; § 73.71

Reporting of safeguards events

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
		The Commission views this length of time as reasonable to accomplish these broader objectives. This reporting requirement does not include a followup written report. The Commission believes that a written report from the licensees would be of minimal value and would be an unnecessary regulatory burden, because the types of incidents to be reported are transitory in nature and time-sensitive. The proposed text would be neither a request for intelligence collection activities nor authority for the conduct of law enforcement or intelligence activities. This paragraph would simply require the reporting of observed activities. The Commission may consider the applicability of this requirement to other types of licensees in future rulemaking.

Table 5 - Proposed Part 73; § 73.71

Reporting of safeguards events

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
(a)(2) This notification must be made to the NRC Operations Center via the Emergency Notification System, if the licensee is party to that system.	(e) The licensees shall make the notifications required by paragraphs (a), (b), (c), and (d) of this section to the NRC Operations Center via the Emergency Notification System, or other dedicated telephonic system that may be designated by the Commission, if the licensee has access to that system.	This requirement would be renumbered and revised as a conforming change to new paragraph (d). Other revisions would include changing the phrase “This notification must be made to” would be replaced by the active-voice phrase “The licensee shall make” to clarify that it would be the licensee who takes the notification action. The phrase “or other dedicated telephonic system that may be designated by the Commission” would be added to allow flexibility to address advances in communications systems.
(a)(2) If the Emergency Notification System is inoperative or unavailable, the licensee shall make the required notification via commercial telephonic service or other dedicated telephonic system or any other methods that will ensure that a report is received by the NRC Operations Center within one hour.	(e)(1) If the Emergency Notification System or other designated telephonic system is inoperative or unavailable, licensees shall make the required notification via commercial telephonic service or any other methods that will ensure that a report is received by the NRC Operations Center within the timeliness requirements of paragraphs (a), (b), (c), and (d) of this section, as applicable.	This requirement would be renumbered and retained with minor revision. The phrase “within one hour” would be replaced with the phrase “within the timeliness requirements of paragraphs (a), (b), (c), and (d) of this section, as applicable.” This would provide consistency with the varying submission intervals for notifications under paragraphs (a) through (d).

Table 5 - Proposed Part 73; § 73.71

Reporting of safeguards events

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
(a)(2) The exemption of Section 73.21(g)(3) applies to all telephonic reports required by this section.	(e)(2) The exception of § 73.21(g)(3) for emergency or extraordinary conditions applies to all telephonic reports required by this section.	This requirement would be renumbered and retained with minor revision to provide clarity [and consistency with § 73.21 safeguards information regulations] on what types of telephonic notifications are exempt from the secure communications requirements of § 73.21.
(a)(3) The licensee shall, upon request to the NRC, maintain an open and continuous communication channel with the NRC Operations Center.	(e)(3) For events reported under paragraph (a) of this section, the licensee may be requested by the NRC to maintain an open, continuous communication channel with the NRC Operations Center, once the licensee has completed other required notifications under this section, § 50.72 of this chapter, or appendix E of part 50 of this chapter and any immediate actions to stabilize the plant. When established, the continuous communications channel shall be staffed by a knowledgeable individual in the licensee's security or operations organizations (e.g., a security supervisor, an alarm station operator, operations personnel, etc.) from a location deemed appropriate by the licensee.	This requirement would be retained and revised into three separate requirements. The first sentence would be reworded to reflect the renumbered event reports under this section. For the 15-minute reports, the paragraph would indicate that a licensee may be requested to establish a "continuous communications channel" following the initial 15-minute notification. The establishment of a continuous communications channel would not supercede current emergency preparedness or security requirements to notify State officials or local law enforcement authorities, nor would it supercede requirements to take immediate action to stabilize the reactor plant (e.g., in response to a reactor scram or to the loss of offsite power).

Table 5 - Proposed Part 73; § 73.71

Reporting of safeguards events

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
	The continuous communications channel may be established via the Emergency Notification System or other dedicated telephonic system that may be designated by the Commission, if the licensee has access to that system, or a commercial telephonic system.	A new requirement would be added for the person communicating to be knowledgeable and from the licensee's security or operations organization. This language would provide licensees with flexibility in choosing personnel to fulfill this communications role and in choosing the location for this communication (e.g., control room, security alarm station, technical support center, etc.). This language would also provide licensees direction and flexibility on the telephonic systems that may be used for this communications channel.
(a)(3) The licensee shall, upon request to the NRC, maintain an open and continuous communication channel with the NRC Operations Center.	(e)(4) For events reported under paragraphs (b) or (c) of this section, the licensee shall maintain an open, continuous communication channel with the NRC Operations Center upon request from the NRC.	This requirement would be renumbered and retained with minor revision to support the renumbering of existing paragraphs (a) and (b) to new (b) and (c).

Table 5 - Proposed Part 73; § 73.71

Reporting of safeguards events

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
	(e)(5) For suspicious events reported under paragraph (d) of this section, the licensee is not required to maintain an open, continuous communication channel with the NRC Operations Center.	This would be a new requirement. For suspicious activity reports, no continuous communication channel would be required. The Commission's view is that because these reports are intended for law enforcement, threat assessment, and intelligence community purposes, rather than event followup purposes, a continuous communications channel is not necessary.
(c) Each licensee subject to the provisions of §§73.20, 73.37, 73.50, 73.51, 73.55, 73.60, or each licensee possessing SSNM and subject to the provisions of §73.67(d) shall maintain a current log . . .	(f) Each licensee subject to the provisions of §§ 73.20, 73.37, 73.50, 73.51, 73.55, 73.60, or each licensee possessing SSNM and subject to the provisions of §73.67(d) shall maintain a current safeguards event log.	This requirement would be renumbered and retained with minor revision. The term "safeguards event" would be added between "current" and "log" to provide greater clarity and consistency with appendix G.

Table 5 - Proposed Part 73; § 73.71

Reporting of safeguards events

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
(c) . . . and record the safeguards events described in Paragraphs II (a) and (b) of appendix G to this part within 24 hours of discovery by a licensee employee or member of the licensee's contract security organization.	(f)(1) The licensee shall record the safeguards events described in paragraph IV of appendix G of this part within 24 hours of discovery.	This requirement would be renumbered and retained with revision. This paragraph would also be revised to reflect the renumbering of appendix G. The language on discovery by a licensee or licensee contractor would be removed to reduce confusion. The Commission expects all logable events to be recorded, irrespective of who identifies the security issue (i.e., recordable events discovered by licensee staff, contractors, NRC or State inspectors, or independent auditors should be logged).
(c) ...The licensee shall retain the log of events recorded under this section as a record for three years after the last entry is made in each log or until termination of the license.	(f)(2) The licensees shall retain the log of events recorded under this section as a record for three (3) years after the last entry is made in each log or until termination of the license.	This requirement would be renumbered and retained with minor revision by adding “(3)” after “three” [years].
(a)(4) The initial telephonic notification must be followed within a period of 60 days by a written report submitted to the NRC by an appropriate method listed in § 73.4.	(g) Written reports. (1) Each licensee making an initial telephonic notification under paragraphs (a), (b), and (c) of this section shall also submit a written report to the NRC within a period of 60 days by an appropriate method listed in § 73.4.	This requirement would be renumbered and retained with revision. The current text would be retained requiring a written 60-day report be submitted for 1-hour notifications under paragraph (b) and (c). A written 60-day report would also be required for 15-minute notifications under paragraph (a).

Table 5 - Proposed Part 73; § 73.71

Reporting of safeguards events

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
	(g)(2) Licenses are not required to submit a written report following a telephonic notification made under paragraph (d) of this section.	This paragraph would be a new requirement. Licensees would not be required to submit a written report for a suspicious activity notification made under paragraph (d) as no ”security event” has occurred. Any followup that might be necessary would be handled through the Commission’s threat assessment procedures.
(d) Each licensee shall submit to the Commission the 60-day written reports required under the provisions of this section that are of a quality that will permit legible reproduction and processing....	(g)(3) Each licensee shall submit to the Commission written reports that are of a quality that will permit legible reproduction and processing.	This requirement would be renumbered and retained. The timing requirement and the quality requirement would be split into paragraph (g)(1) and (g)(3), respectively.
(d) ...[I]f the facility is subject to § 50.73 of this chapter, the licensee shall prepare the written report on NRC Form 366. If the facility is not subject to § 50.73 of this chapter, the licensee shall not use this form but shall prepare the written report in letter format....	(g)(4) Licensees subject to § 50.73 of this chapter shall prepare the written report on NRC Form 366. (g)(5) Licensees not subject to § 50.73 of this chapter, shall prepare the written report in letter format.	These requirements would be renumbered and retained.

Table 5 - Proposed Part 73; § 73.71

Reporting of safeguards events

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
(a)(4) In addition to the addressees specified in § 73.4, the licensee shall also provide one copy of the written report addressed to the Director, Division of Nuclear Security, Office of Nuclear Security and Incident Response.	(g)(6) In addition to the addressees specified in § 73.4, the licensees shall also provide one copy of the written report and any revisions addressed to the Director, Office of Nuclear Security and Incident Response.	This requirement would be renumbered and retained with minor revision. The paragraph would be revised to change the organization within the NRC, that should receive an extra copy of the written, or any revisions to the written report, in addition to the standard submission addresses under § 73.4. The phrase “Director, Division of Nuclear Security” would be replaced with the “Director, Office of Nuclear Security and Incident Response.” to reflect changes within the Office of Nuclear Security and Incident Response and reduce the need for future changes to this regulation with realignment of the NRC’s internal structure.
(a)(4) The report must include sufficient information for NRC analysis and evaluation.	(g)(7) The report must include sufficient information for NRC analysis and evaluation.	This requirement would be retained and be renumbered.

Table 5 - Proposed Part 73; § 73.71

Reporting of safeguards events

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
(a)(5) Significant supplemental information which becomes available after the initial telephonic notification to the NRC Operations Center or after the submission of the written report must be telephonically reported to the NRC Operations Center and also submitted in a revised written report (with the revisions indicated) to the Regional Office and the Document Control Desk.	(g)(8) Significant supplemental information which becomes available after the initial telephonic notification to the NRC Operations Center or after the submission of the written report must be telephonically reported to the NRC Operations Center under paragraph (e) of this section and also submitted in a revised written report (with the revisions indicated) as required under paragraph (g)(6) of this section.	This requirement would be renumbered and revised. Language would be added to clarity the updating of notifications made under paragraph (e) and to require revised written reports. Written initial and revised reports would be submitted in accordance with paragraph (g)(6) of this section.
(a)(5) Errors discovered in a written report must be corrected in a revised report with revisions indicated.	(g)(9) Errors discovered in a written report must be corrected in a revised report with revisions indicated.	This requirement would be renumbered and retained.
(a)(5) The revised report must replace the previous report; the update must be a complete entity and not contain only supplementary or revised information.	(g)(10) The revised report must replace the previous report; the update must be complete and not be limited to only supplementary or revised information.	This requirement would be renumbered and retained with minor grammatical changes.
(a)(5) Each licensee shall maintain a copy of the written report of an event submitted under this section as record for a period of three years from the date of the report.	(g)(11) Each licensee shall maintain a copy of the written report of an event submitted under this section as record for a period of three (3) years from the date of the report.	This requirement would be renumbered and retained with minor revision by adding “(3)” after “three” [years].

Table 5 - Proposed Part 73; § 73.71

Reporting of safeguards events

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
(e) Duplicate reports are not required for events that are also reportable in accordance with §§50.72 and 50.73 of this chapter.	(h) Duplicate reports are not required for events that are also reportable in accordance with §§ 50.72 and 50.73 of this chapter.	This requirement would be retained and be renumbered.

Table 6 - Proposed Part 73, Appendix B

Nuclear Power Reactor Training and Qualification

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
Appendix B to Part 73 General Criteria for Security Personnel	Appendix B to Part 73 VI. Nuclear Power Reactor Training and Qualification Plan	This proposed Paragraph VI and header would be added to the current appendix B to replicate current requirements, ensure continuity between training and qualification programs and requirements for security personnel, and provide for the separation, modification, addition, and clarification of training and qualification requirements as they apply specifically to operating nuclear power reactors.
Introduction	A. General Requirements and Introduction	The phrase "General Requirements and" would be added to this header for formatting purposes.

Appendix B, Introduction, Paragraph 1: Security personnel who are responsible for the protection of special nuclear material on site or in transit and for the protection of the facility or shipment vehicle against radiological sabotage should, like other elements of the physical security system, be required to meet minimum criteria to ensure that they will effectively perform their assigned security-related job duties.	A.1. The licensee shall ensure that all individuals who are assigned duties and responsibilities required to prevent significant core damage and spent fuel sabotage, implement the Commission-approved security plans, licensee response strategy, and implementing procedures, meet minimum training and qualification requirements to ensure each individual possesses the knowledge, skills, and abilities required to effectively perform the assigned duties and responsibilities.	This requirement would retain the requirement for security personnel to meet minimum criteria to ensure that they will effectively perform their assigned security-related job duties. The phrase “security personnel” would be replaced with the phrase “all individuals” to describe the Commission determination that any individual who is assigned to perform a security function must be trained and qualified to effectively perform that security function. The phrase “on site or in transit and for the protection of the facility or shipment vehicle” would be deleted to remove language not applicable to power reactors. The phrase “against radiological sabotage” would be replaced with the phrase "required to prevent core damage and spent fuel sabotage,.” The phrase ”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 training and qualification to satisfy the performance objective for protection against radiological sabotage. The word “should" would be deleted because training and qualification would be required not suggested.

		The phrase “like other elements of the physical security system, be required to meet minimum criteria to ensure that they will effectively perform their assigned security-related job duties” would be replaced with the phrase “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” to describe the Commission determination that minimum training and qualification requirements are met to provide assurance that assigned individuals possess the knowledge, skills, and abilities that are required to effectively perform the assigned function.
Appendix B, Introduction: In order to ensure that those individuals responsible for security are properly equipped and qualified to execute the job duties prescribed for them, the NRC has developed general criteria that specify security personnel qualification requirements.	A.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.	This requirement would retain the requirement for the licensee to ensure that all personnel assigned security duties and responsibilities are properly trained and qualified. The word, “suited” would be added to reflect the suitability requirements of the current appendix B. The word, “trained” would be added to reflect the training requirements of the current appendix B.

		The phrase “responsible for security” would be replaced with the phrase “who are assigned to perform duties and responsibilities required for the implementation of the Commission-approved security plans, licensee response strategy, and implementing procedures” to identify the major programmatic areas from which security duties are derived. The phrase “execute the job duties prescribed for them” would be replaced with the phrase “perform their assigned duties and responsibilities” to for consistency with the updated language used in the proposed rule. The acronym “NRC” would be replaced with the word “Commission” to remove the use of this acronym. The phrase “general criteria that specify security personnel qualification requirements” would be replaced with the phrase “minimum training and qualification requirements” for consistency with the use of the word "minimum" and the phrase "general criteria that specify". The phrase “that shall be implemented through a Commission-approved training and qualification plan” would be added for consistency with the proposed 10 CFR 73.55.

Appendix B, Introduction: These general criteria establish requirements for the selection, training, equipping, testing, and qualification of individuals who will be responsible for protecting special nuclear materials, nuclear facilities, and nuclear shipments. Appendix B, Introduction: When required to have security personnel that have been trained, equipped, and qualified to perform assigned security job duties in accordance with the criteria in this appendix, the licensee must establish, maintain, and follow a plan that shows how the criteria will be met.	A.3. The licensee shall establish, maintain, and follow a Commission-approved training and qualification plan, describing how the minimum training and qualification requirements set forth in this appendix will be met, to include the processes by which all members of the security organization, will be selected, trained, equipped, tested, and qualified.	This requirement for selection, training, equipping, testing, and qualification would be retained and reformatted to combine two current requirements. An expansion of the plan requirements would describe the content of an approved training and qualification plan that would demonstrate how the requirements in the appendix are met.
Appendix B, II.D: Each individual assigned to perform the security related task identified in the licensee physical security or contingency plan shall demonstrate the required knowledge, skill, and ability in accordance with the specified standards for each task as stated in the NRC approved licensee training and qualifications plan.	A.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.	This requirement to demonstrate knowledge, skills would be retained. The requirement to demonstrate knowledge, skills, and abilities prior to assignment would be added to ensure that each individual demonstrates the ability to apply formal classroom training to assigned duties and responsibilities.

Appendix B, Paragraph I.C. ...shall consider job-related functions such as strenuous activity, physical exertion, levels of stress, and exposure to the elements as they pertain to each individual's assigned security job duties for both normal and emergency operations.	A.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.	This requirement would be based upon the current requirement of appendix B, Paragraph I.C., and require that due to changes in the threat environment that personnel must be trained in a manner which simulates the site specific conditions under which the assigned duties and responsibilities are required to be performed.
Appendix B, Introduction: Security personnel who are responsible for the protection of special nuclear material on site or in transit and for the protection of the facility or shipment vehicle against radiological sabotage should, like other elements of the physical security system, be required to meet minimum criteria to ensure that they will effectively perform their assigned security-related job duties.	A.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.	This requirement would be based upon the current appendix B, Introduction. Due to changes to the threat environment, this requirement would identify the applicability of appendix B training and qualification standards to all security-related duties, whether they be performed by traditional security organization personnel or other plant staff. Licensees would be required by the proposed rule to describe how non-security personnel would be trained to perform the specific functions to which they are assigned in accordance with the Commission-approved training and qualification plan, and that non-security personnel would be required to meet the requirements of this proposed appendix that are specifically articulated and necessary to perform the required, specific duty or responsibility assigned.

Appendix B, Paragraph I.E. At least every 12 months, central alarm station operators shall be required to meet the physical requirements of B.1.b of this section, and guards, armed response personnel, and armed escorts shall be required to meet the physical requirements of Paragraphs B.1.b (1) and (2), and C of this section.	A.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.	This annual training requirement would be retained and revised for consistency with the proposed § 73.55. The intent would be to provide regulatory stability and consistency by requiring annual training at a nominal 12 month intervals, while providing for those instances when a licensee may not be able to conduct annual training on the scheduled date due to site specific conditions or unforseen circumstances. This would provide needed flexibility in accomplishing required training. This requirement would provide for annual training to be conducted up to three (3) months prior to, or three (3) months after the scheduled initial date. However, to insure that the required training period would be not repeatedly extended beyond the required 12 months, this requirement would require that the next subsequent training date be 12 months from the originally scheduled date. The intent would be to provide licensees with the necessary flexibility to resolve scheduling issues due to unexpected circumstances such as forced outages, unforseen weather conditions, and ensure that training would be completed within the minimum required frequency.
I. Employment suitability and qualification.	B. Employment suitability and qualification.	This header would be retained without change.

Appendix B, Paragraph I.A. Suitability:	B.1. Suitability.	This header would be retained without change.
Appendix B, Paragraph I.A.1. Prior to employment, or assignment to the security organization, an individual shall meet the following suitability criteria:	B.1.a. Before employment, or assignment to the security organization, an individual shall:	This requirement would be retained with only minor grammatical changes.
Appendix B, Paragraph I.A.1.a. Educational development--Possess a high school diploma or pass an equivalent performance examination designed to measure basic job-related mathematical, language, and reasoning skills, ability, and knowledge, required to perform security job duties.	B.1.a.(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;	This requirement to possess a high school diploma or pass an equivalent performance examination would be retained. The title “Educational development” would be deleted because it would not be needed. The phrase "job-related" would be deleted because it would be addressed by the phrase "required to perform". The word “job” would be replaced with the word “responsibilities” to more accurately reflect the skills required. The word “ability” would be replaced with the word “abilities” to correct grammar.
Appendix B, Paragraph I.A.2. Prior to employment or assignment to the security organization in an armed capacity, the individual, in addition to (a) and (b) above, must be 21 years of age or older.	B.1.a.(2) Have attained the age of 21 for an armed capacity or the age of 18 for an unarmed capacity; and	This age requirement for armed personnel would be retained. The phrase “or the age of 18 for an unarmed capacity” would be added to specify a minimum age since the current NRC approved training and qualification plans for all licensees requires unarmed members to have attained the age of 18 prior to assignment.

Appendix B, Paragraph I.A.1.b. Felony convictions-Have no felony convictions involving the use of a weapon and no felony convictions that reflect on the individual's reliability.	B.1.a.(3) An unarmed individual assigned to the security organization may not have any felony convictions that reflect on the individual's reliability.	The phrase" Have no felony convictions involving the use of a weapon" would be deleted because the proposed rule would address this requirement in 10 CFR 73.18 for an armed member of the security organization. The phrase "An unarmed individual assigned to the security organization may not have any felony convictions" would be added to retain the current requirement for unarmed individuals.
Appendix B, Paragraph II.C. The qualifications of each individual must be documented and attested by a licensee security supervisor.	B.1.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.	The "attested to by a security supervisor" requirement would be retained. The phrase "to perform assigned duties and responsibilities" would be added to clarify the performance standard for documentation. The phrase "by a qualified training instructor" would be added to require that the security supervisor must attest to the fact that the required training for each individual was administered by a qualified instructor and documentation was obtained and properly completed. The word "licensee" would be deleted because a contract security supervisor may attest to an individual's qualification. These changes would better describe the requirement for verification and documentation of training by a supervisor.

Appendix B, Paragraph I.B. Physical and mental qualifications.	B.2. Physical qualifications.	This header would be retained and the two topics separately addressed. The word “mental” is deleted because psychological qualifications are set forth separately.
Appendix B, Paragraph I.B.1. Physical qualifications:	B.2.a. General Physical Qualifications	This header would be retained. The word "General" would be added to indicate that site specific physical qualifications would be applicable if not addressed herein.
Appendix B, Paragraph I.B.1.a. Individuals whose security tasks and job duties are directly associated with the effective implementation of the licensee physical security and contingency plans shall have no physical weaknesses or abnormalities that would adversely affect their performance of assigned security job duties.	B.2.a.(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.	The requirement would be retained. The phrase “tasks and job duties” would be replaced with the phrase “duties and responsibilities” to reflect current language usage. The phrase “licensee physical security and contingency plans” would be replaced with the phrase ”Commission-approved security plans, licensee protective strategy, and implementing procedures” to specify the source of the duties and responsibilities. The phrase "of assigned security job duties" would be deleted because it would be addressed by the phrase "whose duties and responsibilities" at the beginning of this proposed requirement. The phrase “weaknesses or abnormalities” would be replaced with “conditions” to specify that all physical attributes affecting performance should be considered.

Appendix B, Paragraph I.B.1.b. In addition to a. above, guards, armed response personnel, armed escorts, and central alarm station operators shall successfully pass a physical examination administered by a licensed physician. The examination shall be designed to measure the individual's physical ability to perform assigned security job duties as identified in the licensee physical security and contingency plans.	B.2.a.(2) Armed and unarmed members of the security organization shall be subject to a physical examination designed to measure the individual's physical ability to perform assigned duties and responsibilities as identified in the Commission-approved security plans, licensee protective strategy, and implementing procedures.	This physical examination requirement would be retained. Proposed revisions would combine two current requirements, reflect current language usage, and describe the requirement for measuring the individual's physical ability to assure they can perform assigned duties.
Appendix B, Paragraph I.B.1.b. In addition to a. above, guards, armed response personnel, armed escorts, and central alarm station operators shall successfully pass a physical examination administered by a licensed physician.	B.2.a.(3) This physical examination must be administered by a licensed health professional with final determination being made by a licensed physician to verify the individual's physical capability to perform assigned duties and responsibilities.	This physical examination requirement would be retained. Proposed revisions would describe the minimum qualifications of the individual administering the physical examination and separate the professional qualifications that must be met by the individual(s) administering the physical examination and the person making the determination of the individual's physical capability to perform assigned duties.

Appendix B, Paragraph I.B.1.b. Armed personnel shall meet the following additional physical requirements:	B.2.a.(4) The licensee shall ensure that both armed and unarmed members of the security organization 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.	The physical requirements requirement would be retained. Proposed revisions due to changes to the threat environment would describe the minimum physical requirements for both armed and unarmed security personnel. Inclusion of unarmed personnel would be necessary to account for those instances where the two types of security personnel share similar duties and responsibilities required to implement the approved plans and procedures. The requirement would not apply to administrative security staff, such as clerks or secretaries, for the performance of their assigned administrative duties and responsibilities. However, should such personnel, or other non-security personnel be assigned to perform security functions required to implement the Commission-approved security plans and implementing procedures, these personnel must be trained and qualified to perform these duties and possess appropriate vision, hearing, and physical capabilities that are required to effectively perform the assigned duties or responsibilities.
Appendix B, Paragraph I.B.1.b.(1) Vision:	B.2.b. Vision:	This header would be retained.

Appendix B, Paragraph I.B.1.b.(1)(a) 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.	B.2.b.(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.	This requirement would be retained.
Appendix B, Paragraph I.B.1.b.(1)(a) Near visual acuity, corrected or uncorrected, shall be at least 20/40 in the better eye.	B.2.b.(2) Near visual acuity, corrected or uncorrected, shall be at least 20/40 in the better eye.	This requirement would be retained.
Appendix B, Paragraph I.B.1.b.(1)(a) Field of vision must be at least 70 degrees horizontal meridian in each eye.	B.2.b.(3) Field of vision must be at least 70 degrees horizontal meridian in each eye.	This requirement would be retained.
Appendix B, Paragraph I.B.1.b.(1)(a) The ability to distinguish red, green, and yellow colors is required.	B.2.b.(4) The ability to distinguish red, green, and yellow colors is required.	This requirement would be retained.
Appendix B, Paragraph I.B.1.b.(1)(a) Loss of vision in one eye is disqualifying.	B.2.b.(5) Loss of vision in one eye is disqualifying.	This requirement would be retained.
Appendix B, Paragraph I.B.1.b.(1)(a) Glaucoma shall be disqualifying, unless controlled by acceptable medical or surgical means, provided such medications as may be used for controlling glaucoma do not cause undesirable side effects which adversely affect the individual's ability to perform assigned security job duties, and provided the visual acuity and field of vision requirements stated above are met.	B.2.b.(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 job duties, and provided the visual acuity and field of vision requirements stated previously are met.	This requirement would be retained.

Appendix B, Paragraph I.B.1.b.(1)(a) On-the-job evaluation shall be used for individuals who exhibit a mild color vision defect.	B.2.b.(7) On-the-job evaluation must be used for individuals who exhibit a mild color vision defect.	This requirement would be retained.
Appendix B, Paragraph I.B.1.b.(1)(a) If uncorrected distance vision is not at least 20/40 in the better eye, the individual shall carry an extra pair of corrective lenses. Appendix B, Paragraph I.B.1.b.(1)(b) Where corrective eyeglasses are required, they shall be of the safety glass type.	B.2.b.(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.	The vision requirements in Paragraphs I.B.1.b.(1)(a) and I.B.1.b.(1)(b) would be retained and combined. The phrase “in the event that the primaries are damaged” would be added to ensure that the individual would continue to meet minimum vision requirements should one pair be damaged and not usable. The phrase “carry an extra pair of corrective lenses” would include any future technological advancements in vision correction and would include glasses and/or contact lenses, or other materials by any name whose purpose would be to correct an individual’s vision.
Appendix B, Paragraph I.B.1.b.(1)(c) The use of corrective eyeglasses or contact lenses shall not interfere with an individual's ability to effectively perform assigned security job duties during normal or emergency operations.	B.2.b.(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.	This requirement would be retained.
Appendix B, Paragraph I.B.1.b.(2) Hearing:	B.2.c. Hearing:	This header would be retained.

Appendix B, Paragraph I.B.b.(2)(a) Individuals shall have no 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 (by ISO 389 “Standard Reference Zero for the Calibration of Puritone Audiometer" (1975) or ANSI S3.6-1969 R. 1973) “Specifications for Audiometers"). ISO 389 and ANSI S3.6-1969 have been approved for incorporation by reference by the Director of the Federal Register.	B.2.c.(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.	The requirement concerning hearing loss would be retained. Referenced standards would be deleted. The NRC staff has determined that reference to specific calibration standards would no longer be necessary and that it would not be appropriate to require these standards by this proposed rule because such standards may become outdated and obsolete, and equipment may change due to technological advancements, which would require future rule changes to update the referenced documents. The expectation would be that a licensed professional will perform this examination using professionally accepted standards to include calibration standards for equipment used.
Appendix B, Paragraph I.B.1.b.(2)(b) A hearing aid is acceptable provided suitable testing procedures demonstrate auditory acuity equivalent to the above stated requirement.	B.2.c.(2) A hearing aid is acceptable provided suitable testing procedures demonstrate auditory acuity equivalent to the hearing requirement.	This requirement would be retained.
Appendix B, Paragraph I.B.1.b.(2)(c) The use of a hearing aid shall not decrease the effective performance of the individual's assigned security job duties during normal or emergency operations.	B.2.c.(3) The use of a hearing aid may not decrease the effective performance of the individual's assigned security job duties during normal or emergency operations.	This requirement would be retained.

Appendix B, Paragraph I.B.1.b.(3) Diseases -	B.2.d. Existing medical conditions.	This requirement would be revised to require that the licensee consider all existing medical conditions that would adversely effect performance and not limit consideration to only pre-existing conditions or “diseases.”
Appendix B, Paragraph I.B.1.b.(3) ...Individuals shall have no established medical history or medical diagnosis of epilepsy or diabetes, or, where such a condition exists...	B.2.d.(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.	The requirement concerning medical history would be retained. Proposed revisions would require that the licensee consider any existing medical conditions and not limit this consideration to only specified conditions. The phrase “epilepsy or diabetes, or, where such a condition exists” would be replaced with the phrase “existing medical conditions which could interfere with or prevent the individual from effectively performing assigned duties and responsibilities" to state the requirement that the licensee must consider all medical conditions that could adversely affect performance.

Appendix B, Paragraph I.B.1.b.(3) ...the individual shall provide medical evidence that the condition can be controlled with proper medication so that the individual will not lapse into a coma or unconscious state while performing assigned security job duties.	B.2.d.(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.	This requirement to provide medical evidence that a condition can be controlled would be retained. The phrase "proper medication" is replaced with the phrase "medical treatment" to account for conditions that may be treated without medication and future changes in medicine. The phrase "so that the individual will not lapse into a coma or unconscious state while" would be replaced with the phrase "in a manner which does not adversely affect the individual's fitness-for-duty, mental alertness, physical condition, or capability to otherwise effectively" to describe the requirement that the ability to perform duties would be the criteria and not be limited to the current specific conditions of coma or unconscious state. The phrase "job duties" would be replaced with the phrase "duties and responsibilities" to reflect plain language requirements.

Appendix B, Paragraph I.B.1.b.(4) Addiction-Individuals shall have no established medical history or medical diagnosis of habitual alcoholism or drug addiction, or, where such a 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 performing assigned security job duties.	B.2.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.	This requirement regarding addiction would be retained. The word “effectively” would be added to describe the requirement that the individual must be able to carry out tasks in a manner that would provide the necessary results. The phrase “job duties” would be replaced with the phrase "duties and responsibilities” to satisfy plain language requirements.
Appendix B, Paragraph I.B.1.b.(5) 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 security job duties shall, prior to resumption of such duties, provide medical evidence of recovery and ability to perform such security job duties.	B.2.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.	This requirement to provide medical evidence of recovery from an incapacitation would be retained. The phrase “job duties” would be replaced with the phrase "duties and responsibilities” for consistency with other proposed rule and plain language requirements.
Appendix B, Paragraph I.B.2. Mental qualifications:	B.3. Psychological qualifications:	This mental qualifications requirement would be retained. The word “mental” would be replaced by the word “psychological” to be consistent with other proposed changes and plain language requirements.

Appendix B, Paragraph I.B.2.a. Individuals whose security tasks and job duties are directly associated with the effective implementation of the licensee physical security and contingency plans shall demonstrate mental alertness and the capability to exercise good judgment, implement instructions, assimilate assigned security tasks, and possess the acuity of senses and ability of expression sufficient to permit accurate communication by written, spoken, audible, visible, or other signals required by assigned job duties.	B.3.a. Armed and unarmed members of the security organization shall demonstrate the ability to apply good judgment, mental alertness, the capability to implement instructions and assigned tasks, and possess the acuity of senses and ability of expression sufficient to permit accurate communication by written, spoken, audible, visible, or other signals required by assigned duties and responsibilities.	This requirement to demonstrate good judgement, ability to implement instructions/tasks, and to communicate would be retained. The phrase "Individuals whose security tasks and job duties are directly associated with the effective implementation of the licensee physical security and contingency plans" would be replaced with the phrase "Armed and unarmed members of the security organization" to describe the requirement that these mental requirements are minimum standards that must apply to both armed and unarmed security personnel because they share similar duties and responsibilities for the physical protection of the site.
Appendix B, Paragraph I.B.2.b. Armed individuals, and central alarm station operators, in addition to meeting the requirement stated in Paragraph a. above, shall have no emotional instability that would interfere with the effective performance of assigned security job duties. The determination shall be made by a licensed psychologist or psychiatrist, or physician, or other person professionally trained to identify emotional instability.	B.3.b. A licensed clinical psychologist, psychiatrist, or physician trained in part to identify emotional instability shall determine whether armed members of the security organization 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.	The requirement regarding emotional instability would be retained. The phrase "Armed individuals, and central alarm station operators" would be replaced with the phrase "armed members of the security organization and alarm station operators" to refer to both alarm station operators, and for consistency with the terminology used in the proposed rule.

Appendix B, Paragraph I.B.2.b. Armed individuals, and central alarm station operators, in addition to meeting the requirement stated in Paragraph a. above, shall have no emotional instability that would interfere with the effective performance of assigned security job duties. The determination shall be made by a licensed psychologist or psychiatrist, or physician, or other person professionally trained to identify emotional instability.	B.3.c. A person professionally trained to identify emotional instability shall determine whether unarmed members of the security organization in addition to meeting the requirement stated in Paragraph a. of this section, have no emotional instability that would interfere with the effective performance of assigned duties and responsibilities.	Section B.3.c. would be added to describe that these emotional instability requirements are minimum standards that must apply to armed and unarmed security personnel because they share similar duties and responsibilities for the physical protection of the site.
Appendix B, Paragraph I.C. Medical examinations and physical fitness qualifications.	B.4. Medical examinations and physical fitness qualifications.	This header would be retained.
Appendix B, Paragraph I.C. Guards, armed response personnel, armed escorts and other armed security force members shall be given a medical examination including a determination and written certification by a licensed physician that there are no medical contraindications as disclosed by the medical examination to participation by the individual in physical fitness tests.	B.4.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.	This medical examination requirement would be retained. Current requirements for an examination and certification would be reformatted to separate the two requirements in order to specify the requirements for medical examinations and certifications.

Appendix B, Paragraph I.C. Guards, armed response personnel, armed escorts and other armed security force members shall be given a medical examination including a determination and written certification by a licensed physician that there are no medical contraindications as disclosed by the medical examination to participation by the individual in physical fitness tests.	B.4.a. 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.	This requirement for written certification would be retained. Current requirements for an examination and certification would be reformatted to separate the two requirements in order to specify the requirements for medical examinations and certifications. The licensee must obtain and retain a written certification from the licensed physician who performed the examination, which clearly states that the individual has no medical condition that would cause the licensee to doubt the individual's ability to perform the physical requirements of the fitness test and therefore, could not effectively perform assigned duties. The phrase "associated with assigned duties" would be added to require that the test simulates the conditions under which the assigned duties and responsibilities are required to be performed.

Appendix B, Paragraph I.C. Subsequent to this medical examination, guards, armed response personnel, armed escorts and other armed security force members shall demonstrate physical fitness for assigned security job duties by performing a practical physical exercise program within a specific time period.	B.4.b. Before assignment, armed members of the security organization shall demonstrate physical fitness for assigned duties and responsibilities by performing a practical physical fitness test.	This medical examination and physical fitness requirement would be retained. The phrase “guards, armed response personnel, armed escorts and other armed security force members” would be replaced with the phrase “armed members of the security organization“ for consistency with terminology used in the proposed rule. The phrase “security job duties” would be replaced with the phrase “assigned duties and responsibilities” for consistency with terminology used in the proposed rule. The phrase “exercise program” would be replaced with the phrase “practical physical fitness test” for consistency with terminology used in the proposed rule. The term "practical" would mean that the test must be representative of the physical requirements of duties and responsibilities assigned to armed members of the security organization. The phrase “specific time period” would be deleted because specific time periods are delineated in Commission-approved security plans.

Appendix B, Paragraph I.C. The exercise program performance objectives shall be described in the license training and qualifications plan and shall consider job-related functions such as strenuous activity, physical exertion, levels of stress, and exposure to the elements as they pertain to each individual's assigned security job duties for both normal and emergency operations.	B.4.b.(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 job 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.	This requirement related to physical conditions would be retained. The phrase “and shall consider job-related functions such as strenuous activity, physical exertion, levels of stress, and exposure to the elements as they pertain to each individual's assigned security job duties for both normal and emergency operations” is replaced with the phrase "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 job duties for both normal and emergency operations” for consistency with the terminology used by the proposed rule. The phrase "and shall simulate site specific conditions under which the individual will be required to perform assigned duties and responsibilities" would be added to specify that site specific conditions such as facility construction and layout, weather, terrain, elements, should be simulated to the extent reasonably practical.

Appendix B, Paragraph I.C. The exercise program performance objectives shall be described in the license training and qualifications plan...	B.4.b.(2) The licensee shall describe the physical fitness test in the Commission-approved training and qualification plan.	This approved plan requirement would be retained and separated to address this requirement individually. The phrase "The exercise program performance objectives shall be described in the license training and qualifications plan " would be replaced with the phrase "The licensee shall describe the physical fitness test in the Commission-approved training and qualification plan" to reflect plain language requirements.
Appendix B, Paragraph I.C. ...shall consider job-related functions such as strenuous activity, physical exertion, levels of stress, and exposure to the elements as they pertain to each individual's assigned security job duties for both normal and emergency operations.	B.4.d.(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.	This requirement would be based on the current appendix B, Paragraph I.C. and would require that the licensee include, as part of the physical fitness test, performance objectives that are designed to demonstrate the ability of each individual to meet the physical attributes required of assigned duties and responsibilities.

Appendix B, Paragraph I.C. The physical fitness qualification of each guard, armed response person, armed escort, and other security force member shall be documented and attested to by a licensee security supervisor.	B.4.b(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.	This documentation and attesting requirement would be retained. This requirement would be intended to include adequate oversight and verification of qualification while providing flexibility to the licensee to determine how to best use management resources. The phrase “by a qualified training instructor”would be added to specify the training instructor observes and documents that the qualification criteria are met while the security supervisor attests to the fact that the required training for each individual was administered by a qualified instructor and documentation was obtained and properly completed. The word “licensee” would be deleted because the proposed rule would permit a contract security supervisor to attest to an individual’s qualification. The phrase “guard, armed response person, armed escort, and other security force member” would be replaced with the phrase “each armed member of the security organization” for consistency with the terminology used in the proposed rule.
Appendix B, Paragraph I.E. Physical requalification --	B.5. Physical requalification.	This header would be retained.

Appendix B, Paragraph I.E. At least every 12 months, central alarm station operators shall be required to meet the physical requirements of B.1.b of this section, and guards, armed response personnel, and armed escorts shall be required to meet the physical requirements of Paragraphs B.1.b (1) and (2), and C of this section.	B.5.a. At least annually, armed and unarmed members of the security organization shall be required to demonstrate the capability to meet the physical requirements of this appendix and the licensee training and qualification plan.	This requirement to demonstrate the capability to meet the physical requirements would be retained. The phrase “every 12 months” would be replaced with the word “annually” to specify that annual requirements must be scheduled at a nominal 12 month periodicity but may be conducted up to three (3) months prior to three (3) months after the scheduled date with the next scheduled date 12 months from the originally scheduled date. This requirement would be intended to provide flexibility to the licensee to account for those instances when site specific conditions, such as outages, preclude conducting requalification at the scheduled dates, while ensuring that the intent of the requirement would be still met without requiring the next scheduled date to be changed to correspond with the month in which the requalification is performed.

Appendix B, Paragraph I.E. The physical fitness qualification of each guard, armed response person, armed escort, and other security force member shall be documented and attested to by a licensee security supervisor.	B.5.b. The physical requalification of each armed and unarmed member of the security organization must be documented by a qualified training instructor and attested to by a security supervisor.	This documentation and attesting requirement would be retained. This requirement would be intended to include adequate oversight and verification of qualification while providing flexibility to the licensee to determine how to best use management resources. The phrase “by a qualified training instructor” would be added to specify the training instructor observes and documents that the qualification criteria is met while the security supervisor attests to the fact that the required documentation is retained and properly completed. The phrase “guard, armed response person, armed escort, and other security force member” would be replaced with the phrase ”each armed and unarmed member of the security organization” for consistency with the terminology used in the proposed rule. The word “licensee” would be deleted because the proposed rule would permit a contract security supervisor attest to an individual’s qualification.
II. Training and qualifications.	C. Duty training	This new header would be added to provide a section under which the current and proposed non-weapons-related training requirements may be grouped.

Appendix B, Paragraph II.A. Training requirements. Each individual who requires training to perform assigned security-related job tasks or job duties as identified in the licensee physical security or contingency plans shall, prior to assignment, be trained to perform these tasks and duties in accordance with the licensee or the licensee's agent's documented training and qualifications plan. Appendix B, Paragraph II.B. Qualification requirement. Each person who performs security-related job tasks or job duties required to implement the licensee physical security or contingency plan shall, prior to being assigned to these tasks or duties, be qualified in accordance with the licensee's NRC-approved training and qualifications plan.	C.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.	This training requirement would be retained and revised to combine the two current requirements of appendix B, Paragraph II.A. and II.B. This requirement would account for those instances where the licensee may use, in addition to members of the security organization, site personnel from outside of the security organization to perform security related duties, such as, but not limited to, escorts, tampering, detection, and compensatory measures. The Commission views are that security personnel must obtain the requisite knowledge, skills, and abilities of all security-related duties prior to unsupervised assignment.

Appendix B, Paragraph II.D. The areas of knowledge, skills, and abilities that shall be considered in the licensee's training and qualifications plan are as follows: [NOTE: The list of one hundred specific training subjects is omitted here for conservation of space.]	C.1.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.	This requirement would be retained and revised to replace the current list of 100 topic areas with a requirement for the licensee to provide a site specific list in the approved security plans and specify assigned duties in the training and qualification plan. The Commission has determined that the current list would no longer be necessary to ensure that the listed topic areas are addressed by each licensee. In accordance with this proposed appendix, all licensees are required to ensure that all personnel are trained and qualified to perform their assigned duties and responsibilities. Those requirements would encompass topics that are currently listed, making it unnecessary to specifically list the 100 areas of knowledge, skills, and abilities.
Appendix B, Paragraph II.A. Each individual who requires training to perform assigned security-related job tasks or job duties as identified in the licensee physical security or contingency plans shall, prior to assignment, be trained to perform these tasks and duties in accordance with the licensee or the licensee's agent's documented training and qualifications plan.	C.1.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.	This training requirement would be retained. The requirement would specify training of all individuals assigned to perform security functions required to implement the Commission-approved security plans, licensee response strategy, and implementing procedures. The phrase “requires training to perform assigned security-related job tasks or job duties as” would be replaced with the phrase “is assigned duties and responsibilities” to reflect changes to terminology used. The phrase “in the

		licensee physical security or contingency” would be replaced with the phrase “Commission-approved security plans, licensee protective strategy, and implementing procedures” to reflect changes to terminology used. The phrase “these tasks and duties” would be replaced with the phrase "assigned duties and responsibilities" to reflect changes to terminology used. The phrase “licensee or the licensee's agent's documented training and qualifications plan” would be replaced with the phrase “requirements of this appendix and the Commission-approved training and qualification plan” to reflect changes to terminology used.

Appendix B, Paragraph II.B. Each person who performs security-related job tasks or job duties required to implement the licensee physical security or contingency plan shall, prior to being assigned to these tasks or duties, be qualified in accordance with the licensee's NRC-approved training and qualifications plan.	C.1.b. (2) meet the minimum qualification requirements of this appendix and the Commission-approved training and qualification plan.	This qualification requirement would be retained. The requirement would specify the qualification standard for all individuals assigned to perform security functions required to implement the Commission-approved security plans, licensee response strategy, and implementing procedures. The phrase “be qualified in accordance with” would be replaced with the phrase “meet the minimum qualification requirements of this appendix and” to specify that the approved T&Q plan implements the requirements of this proposed rule. The phrase “licensee’s NRC-approved” would be replaced with the phrase “Commission approved” to reflect changes to terminology used.
Appendix B, Paragraph II. A. Training Requirements - Each individual who requires training to perform assigned security - related job tasks or job duties as identified in the licensee physical security or contingency plans shall, prior to assignment, be trained to perform these tasks and duties in accordance with the licensee or licensee’s agent’s documented training and qualification plan.	C.1.b. (3) be trained and qualified in the use of all equipment or devices required to effectively perform all assigned duties and responsibilities.	This requirement would be based on the current appendix B, Paragraph II.A. and specify the requirement for training in the use of equipment required to effectively perform all assigned duties and responsibilities. The Commission views this as facilitating the performance objective of the proposed § 73.55 B.1.

	C.2. On-the-job training	This new header would be added for consistency with the format of this proposed paragraph. This new topic area would be intended to specify the requirement that the licensee training and qualification program must include an on-the-job training program to ensure that assigned personnel have demonstrated an acceptable level of performance and proficiency within the actual work environment, prior to assignment to an unsupervised position.

Appendix B, Paragraph II. A. Training Requirements - Each individual who requires training to perform assigned security - related job tasks or job duties as identified in the licensee physical security or contingency plans shall, prior to assignment, be trained to perform these tasks and duties in accordance with the licensee or licensee's agent's documented training and qualification plan. Appendix B, Paragraph I.B.1.b.(1)(a) On-the-job evaluation shall be used for individuals who exhibit a mild color vision defect.	C.2.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.	This new requirement would be based on the current appendix B, Paragraph II.A. and would specify the requirement that the licensee include on-the-job training as part of the training and qualification program to ensure each individual demonstrates, in an on-the-job setting, an acceptable level of performance and proficiency to carry-out assigned duties and responsibilities prior to an assignment. The expectation would be that on-the-job training would be conducted by qualified security personnel who will observe the trainee's performance and provide input for improvement and final qualification of the trainee and allow each individual to develop and apply, in a controlled but realistic training environment, the knowledge, skills, and abilities presented in formal and informal classroom settings. This requirement would be in addition to licensee specific classroom training that may include instruction on security practices and theory and other training activities for security-related duties.

Appendix B, Paragraph II. A. Training Requirements - Each individual who requires training to perform assigned security - related job tasks or job duties as identified in the licensee physical security or contingency plans shall, prior to assignment, be trained to perform these tasks and duties in accordance with the licensee or licensee's agent's documented training and qualification plan.	C.2.b. In addition to meeting the requirement stated in paragraph C.2.a., before assignment, individuals 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 duties and responsibilities in accordance with the approved 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.	This new requirement would be based on the current appendix B, Paragraph II.A. and would specify the requirement for on-the-job training. This requirement would specify that 40 hours is the minimum time for practical skill development and performance demonstration necessary to fully assess an individual's knowledge, skills, and abilities to effectively carry-out assigned duties and responsibilities prior to assignment to an unsupervised position. This requirement would be in addition to formal and informal classroom instruction. The phrase "by a qualified training instructor" would be added to require that the security supervisor must attest to the fact that the required training for each individual was administered by a qualified instructor and documentation was obtained and properly completed.
Appendix B, Paragraph I.B.1.b.(1)(a) On-the-job evaluation shall be used for individuals who exhibit a mild color vision defect. Appendix B, Paragraph I.C. The exercise program performance objectives shall be described in the license training and qualifications plan and shall consider job-related functions such as strenuous activity, physical exertion, levels of stress, and exposure to the elements as they pertain to each	C.2.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.	This new requirement would be based on the current requirements appendix B, Paragraph II.A. and appendix B, Paragraph II.D. This requirement would provide a list of minimum generic topics which are applicable to all sites and must be addressed, but are not intended to limit the licensee such that site specific topics are not also included. This requirement would also specify that the licensee identify and document in the training and qualification plan, the specific knowledge, skills, and abilities

individual's assigned security job duties for both normal and emergency operations. Appendix B, Paragraph II. A. Training Requirements - Each individual who requires training to perform assigned security - related job tasks or job duties as identified in the licensee physical security or contingency plans shall, prior to assignment, be trained to perform these tasks and duties in accordance with the licensee or licensee's agent's documented training and qualification plan. Appendix B, Paragraph II.D. The areas of knowledge, skills, and abilities that shall be considered in the licensee's training and qualifications plan are as follows: [NOTE: The list of one hundred specific training subjects is omitted here for conservation of space.]	(8) Communications (primary and alternate). (9) Use of assigned equipment. (10) Target sets. (11) Table top drills. (12) Command and control duties.	required by each individual to perform their assigned duties and responsibilities and would generically include any specific items that are currently listed in the current appendix B, Paragraph II.D., and therefore, would require that any applicable topics from the deleted list are addressed.
	C.3. Tactical response team drills and exercises.	This new header would be added for formatting.

Appendix B, Paragraph II. A. Training Requirements - Each individual who requires training to perform assigned security - related job tasks or job duties as identified in the licensee physical security or contingency plans shall, prior to assignment, be trained to perform these tasks and duties in accordance with the licensee or licensee's agent's documented training and qualification plan.	C.3.a. Licensees shall demonstrate response capabilities through a performance evaluation program as described in appendix C to this part.	This requirement would be based on the current appendix B, Paragraph II.A. Due to changes in the threat environment, the requirement would specify that the licensee develop and follow a performance evaluation program designed to demonstrate the effectiveness of the onsite response capabilities.
Appendix B, Paragraph II. A. Training Requirements - Each individual who requires training to perform assigned security - related job tasks or job duties as identified in the licensee physical security or contingency plans shall, prior to assignment, be trained to perform these tasks and duties in accordance with the licensee or licensee's agent's documented training and qualification plan.	C.3.b. The licensee shall conduct drills and exercises in accordance with Commission-approved security plans, licensee protective strategy, and implementing procedures.	This requirement would be based on the current appendix B, Paragraph II.A. Due to changes in the threat environment, the requirement would specify that the licensee conduct drills and exercises to demonstrate the effectiveness of security plans, licensee protective strategy, and implementing procedures.
Appendix B, Paragraph II. A. Training Requirements - Each individual who requires training to perform assigned security - related job tasks or job duties as identified in the licensee physical security or contingency plans shall, prior to assignment, be trained to perform these tasks and duties in accordance with the licensee or licensee's agent's documented training and qualification plan.	C.3.b.(1) Drills and exercises must be designed to challenge participants in a manner which requires each participant to demonstrate requisite knowledge, skills, and abilities.	This requirement would be based on the current appendix B, Paragraph II.A. Due to changes in the threat environment, the requirement would specify that the licensee conduct drills and exercises that are designed to demonstrate each participants requisite knowledge, skills, and abilities to perform security responsibilities.

Appendix B, Paragraph II. A. Training Requirements - Each individual who requires training to perform assigned security - related job tasks or job duties as identified in the licensee physical security or contingency plans shall, prior to assignment, be trained to perform these tasks and duties in accordance with the licensee or licensee's agent's documented training and qualification plan.	C.3.b.(2) Tabletop exercises may be used to supplement drills and exercises to accomplish desired training goals and objectives.	This requirement would be based on the current appendix B, Paragraph II.A. Due to changes in the threat environment, the requirement would convey the Commission view that licensees may use tabletop exercises to supplement drills and exercises as a means of achieving training goals and objectives.
	D. Duty qualification and requalification	This new header would be added for formatting purposes. The word "duty" would be used to clarify that the following sections relate to non-weapons training topics.
	D.1. Qualification demonstration	This new header would be added for formatting purposes.
§ 73.55(b)(4)(i) Upon the request of an authorized representative of the Commission, the licensee shall demonstrate the ability of the physical security personnel to carry out their assigned duties and responsibilities.	D.1.a. Armed and unarmed members of the security organization 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.	This requirement would be based on the current requirement of 10 CFR 73.55(b)(4)(i). Due to changes in the threat environment, it is the Commission's view that licensees must be able to demonstration the ability of security personnel to carry out their assigned duties and responsibilities.

§ 73.55(b)(4)(i) Upon the request of an authorized representative of the Commission, the licensee shall demonstrate the ability of the physical security personnel to carry out their assigned duties and responsibilities.	D.1.b. This demonstration must include an annual written exam and hands-on performance demonstration.	This requirement would be based on the current requirement of 10 CFR 73.55(b)(4)(i) and would specify a licensee requirement to perform written examinations and hands-on performance tests to demonstrate knowledge of the skill or ability being tested. The Commission's view is that written examinations and hands-on performance tests are two components that are necessary to demonstrate the overall qualification and proficiency of an individual performing security duties.

§ 73.55(b)(4)(i) Upon the request of an authorized representative of the Commission, the licensee shall demonstrate the ability of the physical security personnel to carry out their assigned duties and responsibilities.	(1) Written Exam. 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 Demonstration. Armed and unarmed members of the security organization 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.	This requirement would be based on the current requirement of 10 CFR 73.55(b)(4)(i). Due to changes in the threat environment, the rule would require a minimum exam score of 80 percent using accepted training and evaluation techniques. The Commission has determined that a score of 80 percent demonstrates the minimum level of understanding and familiarity of the material acceptable and would be consistent with minimum scores commonly accepted throughout the Nuclear Industry.

73.55(b)(4)(i) Upon the request of an authorized representative of the Commission, the licensee shall demonstrate the ability of the physical security personnel to carry out their assigned duties and responsibilities.	D.1.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.	This requirement would be based upon the current requirement of 10 CFR 73.55(b)(4)(i) and would include, upon request, that an individual assigned security duties or responsibilities demonstrate knowledge, skills and abilities required for such assignments or responsibilities. This requirement would be distinct from the required annual written demonstration above and would be necessary for regulatory consistency. This rule would require that any individual who is assigned to perform any security-related duty or responsibility must demonstrate their capability to effectively perform those assigned duties or responsibilities when requested, regardless of the individual's specific organizational affiliation. These demonstrations would provide the Commission with independent verification and validation that individuals can actually perform their assigned security duties.
Appendix B, Paragraph II.E. Requalification -	D.2. Requalification.	This header would be retained.

Appendix B, Paragraph II.E. Security personnel shall be requalified at least every 12 months to perform assigned security-related job tasks and duties for both normal and contingency operations. Appendix B, Paragraph II.E. Requalification shall be in accordance with the NRC-approved licensee training and qualifications plan.	D.2.a. Armed and unarmed members of the security organization shall be requalified at least annually in accordance with the requirements of this appendix and the Commission-approved training and qualification plan.	This requalification requirement would be retained and revised to combine two requirements of the current appendix B, Paragraph II.E. The rule would require that armed and unarmed members of the security organization must be requalified annually to demonstrate that each individual continues to be capable of effectively performing assigned duties and responsibilities. The phrase "Security personnel" would be replaced with the phrase "Armed and unarmed members of the security organization" for consistency with the proposed rule. The phrase "every 12 months" would be replaced with the word "annual" for consistency with the proposed rule.
Appendix B, Paragraph II.E. The results of requalification must be documented and attested by a licensee security supervisor.	D.2.b. The results of requalification must be documented by a qualified training instructor and attested by a security supervisor.	The requalification requirement would be retained. The proposed rule would require that the licensee provide adequate oversight and verification of qualification process. The phrase "by a qualified training instructor" would be added to specify that the training instructor observes and documents that qualification criteria is met while the security supervisor attests to the fact that the required documentation is retained and properly completed. The word "licensee" would be deleted to

		provide flexibility to the licensee to determine the best use of management resources and to specify that contract security supervisors may be used to satisfy this requirement.
III. Weapons training and Qualification.	E. Weapons training.	This header would be retained and revised. The word “Qualification” would be deleted because "qualification" is addressed individually in this proposed rule.
	E.1. General firearms training.	This new header is added for formatting purposes.
Appendix B, Paragraph III.A. Guards, armed response personnel and armed escorts requiring weapons training to perform assigned security related job tasks or job duties shall be trained in accordance with the licensees' documented weapons training programs.	E.1.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.	This training requirement would be retained and revised to specify that the training be conducted in accordance with the appendix and training and qualification plans. The phrase “Guards, armed response personnel and armed escorts” would be replaced with the phrase “Armed members of the security organization” for consistency with language used in the proposed rule. The phrase “requiring weapons training to perform assigned security related job tasks or job duties” would be deleted

		because that requirement is implied in the proposed rule language. The phrase “licensees' documented weapons training programs” would be replaced with the phrase “Commission-approved training and qualification plan” for consistency with language used in the proposed rule.
	E.1.b. Firearms instructors.	This new header would be added for formatting purposes.
Appendix B, Paragraph III.A. Each individual shall be proficient in the use of his assigned weapon(s) and shall meet prescribed standards in the following areas:	E.1.b.(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, qualification scores, assembly, disassembly, cleaning, storage, handling, clearing, loading, unloading, and reloading, for each assigned weapon.	This requirement would be based on the current appendix B, Paragraph III.A. and would be revised to incorporate current requirements in approved training and qualification plans.
Appendix B, Paragraph III.A. Each individual shall be proficient in the use of his assigned weapon(s) and shall meet prescribed standards in the following areas:	E.1.b.(2) Firearms instructors shall be certified from a national or state recognized entity.	This requirement would be based on the current appendix B, Paragraph III.A. and revised to require that licensees only use certified instructors. It is the Commission view that certification would be required from a national or state recognized entity such as Federal, State military or nationally recognized entities such as National Rifle Association (NRA), International Association of Law Enforcement Firearms Instructors (IALEFI).

Appendix B, Paragraph III.A. Each individual shall be proficient in the use of his assigned weapon(s) and shall meet prescribed standards in the following areas:	E.1.b.(3) Certification must specify the weapon or weapon type(s) for which the instructor is qualified to teach.	This requirement would be based on the current appendix B, Paragraph III.A. and revised to establish minimum standards for those conducting firearms instruction. This requirement would not intend that each firearm instructor be certified on the different manufacturers or brands, but rather that certification be obtained by weapon type such as handgun, shotgun, rifle, machine gun, or other enhanced weapons since each type requires different skills and abilities.
Appendix B, Paragraph III.A. Each individual shall be proficient in the use of his assigned weapon(s) and shall meet prescribed standards in the following areas:	E.1.b.(4) Firearms instructors shall be recertified in accordance with the standards recognized by the certifying national or state entity, but in no case shall re-certification exceed three (3) years.	This requirement would be based upon the current appendix B, Paragraph III.A. and revised to establish minimum standards for those conducting firearms instruction. Firearms instructor skills are perishable and therefore the proposed rule would require periodic re-qualification to demonstrate proficiency. The Commission has determined that three (3) years is a commonly accepted interval for re-certification throughout the firearms community.

Appendix B, Paragraph IV. Qualification firing for the handgun and the rifle must be for daylight firing, and each individual shall perform night firing for familiarization with assigned weapon(s). Appendix B, Paragraph IV. Each individual shall be requalified at least every 12 months.	E.1.c. Annual firearms familiarization. The licensee shall conduct annual firearms familiarization training in accordance with the Commission-approved training and qualification plan.	This requirement would be based upon the current appendix B, Paragraph IV. Due to changes in the threat environment, the Commission seeks to establish minimum standards for weapons familiarization. This requirement would require individuals receive basic firearms familiarization and skills training with each weapon type such as nomenclature, stance, grip, sight alignment, sight stance, grip, sight alignment, sight picture, trigger squeeze, safe handling, range rules, prior to participating in a qualifying course of fire. The specifics of the familiarization must be included in the Commission-approved plan.
Appendix B, Paragraph III.A. Each individual shall be proficient in the use of his assigned weapon(s) and shall meet prescribed standards in the following areas: 1. Mechanical assembly, disassembly, range penetration capability of weapon, and bull's-eye firing. 2. Weapons cleaning and storage. 3. Combat firing, day and night. 4. Safe weapons handling.	E.1.d. The Commission-approved training and qualification plan shall include, but is not limited to, the following areas: (1) Mechanical assembly, disassembly, range penetration capability of weapon, and bull's-eye firing. (2) Weapons cleaning and storage. (3) Combat firing, day and night. (4) Safe weapons handling. (5) Clearing, loading, unloading, and reloading. (6) When to draw and point a weapon.	This proposed rule would retain the current standards listed in appendix B, Paragraph III.A as weapons training areas to be addressed in the Commission-approved T&Q plan. Due to changes in the threat environment, it is the Commission view that additional areas of demonstrated weapon proficiency should be added to the current regulations. The proposed rule would require an individual demonstrate proficiency in the following areas target engagement, weapon malfunctions, cover and

reloading. 5. Clearing, loading, unloading, and 6. When to draw and point a weapon. 7. Rapid fire techniques. 8. Close quarter firing. 9. Stress firing. 10. Zeroing assigned weapon(s).	(7) Rapid fire techniques. (8) Closed quarter firing. (9) Stress firing. (10) Zeroing assigned weapon(s) (sight and sight/scope adjustments). (11) Target engagement. (12) Weapon malfunctions. (13) Cover and concealment. (14) Weapon transition between strong (primary) and weak (support) hands. (15) Weapon familiarization.	concealment weapon transition between strong (primary) and weak (support) hands, and weapon familiarization (areas 11 through 15.)
Appendix B, Paragraph II.D. Security knowledge, skills, and abilities--Each individual assigned to perform the security related task identified in the licensee physical security or contingency plan shall demonstrate the required knowledge, skill, and ability in accordance with the specified standards for each task as stated in the NRC approved licensee training and qualifications plan. The areas of knowledge, skills, and abilities that shall be considered in the licensee's training and qualifications plan are as follows: The use of deadly force.	E.1.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.	The requirements of appendix B, Paragraph II.D. would be modified to clarify training requirements regarding the use of deadly force. The proposed rule would specify that the substance of training in the use of deadly force should be focused on applicable state laws.

Appendix B, Paragraph IV.D. Individuals shall be weapons requalified at least every 12 months in accordance with the NRC approved licensee training and qualifications plan, and in accordance with the requirements stated in A, B, and C of this section.	E.1.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.	This requirement would be based upon the current requalification requirements stated in appendix B, Paragraph IV.D., It is the Commission view that the proposed rule, requiring weapons range activities, would ensure individuals maintain proficiency in the use of assigned weapons and associated perishable skills.
IV. Weapons qualification and requalification program.	F. Weapons qualification and requalification program.	This header would be retained.
	F.1. General weapons qualification requirements.	This header would be added for formatting purposes.
Appendix B, Paragraph IV. Qualification firing for the handgun and the rifle must be for daylight firing, and each individual shall perform night firing for familiarization with assigned weapon(s).	F.1.a. Qualification firing must be accomplished in accordance with Commission requirements and the Commission-approved training and qualification plan for assigned weapons.	The requirement would retain the qualification requirements stated in appendix B, Paragraph IV. The proposed rule would specify that such qualifications have to be accomplished in accordance with Commission-approved training and qualification plans.
The results of weapons qualification and requalification must be documented by the licensee or the licensee's agent.	F.1.b. The results of weapons qualification and requalification must be documented and retained as a record.	This weapons qualification and requalification requirement would be retained. The word “must” would be replaced with the word “shall” for consistency with this proposed rule. The phrase "by the licensee or the licensee's agent" would be replaced with the phrase "and retained as a record" for consistency with the terminology used in the proposed rule.

Each individual shall be requalified at least every 12 months.	F.1.c. Each individual shall be re-qualified at least annually.	This requalification requirement would be retained. The phrase “every 12 months” would be replaced with the word “annually” for consistency with this proposed rule.
Energy Policy Act of 2005	F.2. Alternate weapons qualification. Upon written request by the licensee, the Commission may authorize an applicant or licensee to provide firearms qualification programs other than those listed in this appendix if the applicant or licensee demonstrates that the alternative firearm qualification program satisfies Commission requirements. Written requests must provide details regarding the proposed firearms qualification programs and describe how the proposed alternative satisfies Commission requirements.	This new requirement would be added for consistency with the proposed § 73.19. The proposed rule would require the licensee to request NRC authorization to implement alternative firearms qualification programs pursuant to the licencee’s request for authorization to use “enhanced weapons” as defined in the proposed § 73.19.
Appendix B, Paragraph IV. Qualification firing for the handgun and the rifle must be for daylight firing, and each individual shall perform night firing for familiarization with assigned weapon(s).	F.3. 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 qualification and re-qualification courses for each firearm must describe the performance criteria needed, to include the site specific conditions (such as lighting, elevation, fields-of-fire) under which	This requirement would be based upon the current qualification requirement in appendix B, Paragraph IV. Due to changes to the threat environment, the proposed rule would require that the licensee develop and implement a site specific firearms qualification program and other tactical training to simulate site conditions under which the protective strategy will be implemented. The examples given (lighting, elevation and fields-of fire) are intended to be neither all inclusive nor limiting.

	assigned personnel shall be required to carry-out their assigned duties.	
Appendix B, Paragraph IV. Qualification firing for the handgun and the rifle must be for daylight firing, and each individual shall perform night firing for familiarization with assigned weapon(s).	F.4. Firearms qualification courses. The licensee shall conduct the following qualification courses for weapons used.	This requirement would be based upon the current qualification requirements in appendix B, Paragraph IV. The proposed rule would specify performance expectations for weapons courses.
Appendix B, Paragraph IV. Qualification firing for the handgun and the rifle must be for daylight firing, and each individual shall perform night firing for familiarization with assigned weapon(s). Appendix B, Paragraph IV.A. Handgun - Guards, armed escorts and armed response personnel shall qualify with a revolver or semiautomatic pistol firing the national police course, or an equivalent nationally recognized course. Appendix B, Paragraph IV.B. Semiautomatic Rifle-Guards, armed escorts and armed response personnel, assigned to use the semiautomatic rifle by the licensee training and qualifications plan, shall qualify with a semiautomatic rifle by firing the 100-yard course of fire specified in section 17.5(1) of the National Rifle Association, High Power Rifle Rules book (effective March 15, 1976), (1) or a nationally recognized equivalent course of fire.	F.4.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.	This requirement would combine the current appendix B, Paragraph IV.A., B., and C. Because of changes to the threat environment, it is the Commission view that a higher qualification percentage is required. The Commission has determined that among law enforcement authorities, 70 percent is a commonly accepted fire qualification value requirement for handguns and shotguns and that 80 percent is the commonly accepted value for semi-automatic and enhanced weapons. The proposed rule would increase the acceptable level of proficiency to 70 percent for handgun and shotgun, and 80 percent for the semi-automatic rifle and enhanced weapons.

Appendix B, Paragraph IV.C. Shotgun-Guards, armed escorts, and armed response personnel assigned to use the 12 gauge shotgun by the licensee training and qualifications plan shall qualify with a full choke or improved modified choke 12 gauge shotgun firing the following course:		
Appendix B, Paragraph IV. Qualification firing for the handgun and the rifle must be for daylight firing, and each individual shall perform night firing for familiarization with assigned weapon(s).	F.4.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.	This requirement would combine the qualification standards stated in the current appendix B, Paragraph IV.A., B., and C. Because of changes to the threat environment, it is the Commission view that a higher qualification percentage is required. The Commission has determined that among law enforcement authorities, 70 percent is a commonly accepted night fire qualification value requirement for handguns and shotguns and that, under the same conditions, 80 percent is the commonly accepted

		value for semi-automatic and enhanced weapons. The proposed rule would increase the Night Fire qualification score from familiarization in the current rule, to an acceptable level of proficiency of 70 percent for handgun and shotgun, and 80 percent for the semi-automatic rifle and enhanced weapons.
Appendix B, Paragraph IV. Qualification firing for the handgun and the rifle must be for daylight firing, and each individual shall perform night firing for familiarization with assigned weapon(s).	F.4.c. Annual tactical qualification course. Qualifying score must be an accumulated total of 80 percent of the maximum obtainable score.	This requirement would combine the current qualification requirements in appendix B, Paragraph IV.A., B., and C. In the proposed rule, the annual tactical course of fire would be developed and implemented to simulate the licensee protective strategy in accordance with the Commission-approved training and qualification plan. Licensees would not be not required to include every aspect of its site protective strategy into one tactical course of fire. Instead, licensees should periodically

		evaluate and change their tactical course of fire to incorporate different or changed elements of the site protective strategy so that armed security personnel are exposed to multiple and different site contingency scenarios. In the current threat environment, LLEA tactical teams typically require a minium qualification score of 80 percent to ensure that a higher percentage of rounds hit the intended target to neutralize the threat. This correlates to licensee protective strategies in which a higher percentage of rounds that hit the intended target increase the ability of the security force to neutralize the adversarial threat to prevent radiological sabotage. As a result, the proposed rule would specify 80 percent as the minimum acceptable qualification score for the Tactical Qualification Course.
	F.5. Courses of fire	This heading would be added to clarify the subsequent information and to be consistent with the remainder of this appendix.
Appendix B, Paragraph IV.A. Handgun--	F.5.a. Handgun.	This heading would be brought forward from current rule and would be renumbered accordingly.

Appendix B, Paragraph IV.A Guards, armed escorts and armed response personnel shall qualify with a revolver or semiautomatic pistol firing the national police course, or an equivalent nationally recognized course.	F.5.a.(1) 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 and scores established by a law enforcement course, or an equivalent nationally recognized course.	The qualification requirement would be retained. The phrase “national police course” would be replaced with “law enforcement course” for consistency with the terminology used nationally in reference to firearms standards and courses.
Appendix B, Paragraph IV.A Qualifying score shall be an accumulated total of 70 percent of the maximum obtainable score.	F.5.a.(2) Qualifying scores must be an accumulated total of 70 percent of the maximum obtainable target score.	This requirement would be brought forward from current rule and would be renumbered accordingly.
Appendix B, Paragraph IV.B. Semiautomatic Rifle --	F.5.b. Semiautomatic rifle.	This header would be retained.
Appendix B, Paragraph IV.B. Guards, armed escorts and armed response personnel, assigned to use the semiautomatic rifle by the licensee training and qualifications plan, shall qualify with a semiautomatic rifle by firing the 100-yard course of fire specified in Section 17.5(1) of the National Rifle Association, High Power Rifle Rules book (effective March 15, 1976), (1) or a nationally recognized equivalent course of fire.	F.5.b.(1) Armed members of the security organization, assigned duties and responsibilities involving the use of a semiautomatic rifle shall qualify in accordance with the standards and scores established by a law enforcement course, or an equivalent nationally recognized course.	The qualification requirement would be retained. The phrase “national police course” would be replaced with “law enforcement course” for consistency with the terminology used nationally in reference to firearms standards and courses.
Qualifying score shall be an accumulated total of 80 percent of the maximum obtainable score.	F.5.b.(2) Qualifying scores must be an accumulated total of 80 percent of the maximum obtainable score.	This requirement would be retained.
Appendix B, Paragraph IV.C. Shotgun- -	F.5.c. Shotgun.	This header would be retained.

Appendix B, Paragraph IV.C. Guards, armed escorts, and armed response personnel assigned to use the 12 gauge shotgun by the licensee training and qualifications plan shall qualify with a full choke or improved modified choke 12 gauge shotgun firing the following course:	F.5.c.(1) Armed members of the security organization, assigned duties and responsibilities involving the use of a shotgun shall qualify in accordance with standards and scores established by a law enforcement course, or an equivalent nationally recognized course.	The qualification requirement would be retained. The phrase “national police course” would be replaced with “law enforcement course” for consistency with the terminology used nationally in reference to firearms standards and courses. The phrase “12 gauge” would be deleted to account for future changes and because this specific requirement would be no longer needed in this proposed appendix.
Appendix B, Paragraph IV.C. To qualify the individual shall be required to place 50 percent of all pellets (36 pellets) within the black silhouette.	F.5.c.(2) Qualifying scores must be an accumulated total of 70 percent of the maximum obtainable target score.	The qualification requirement would be retained. Due to changes in the threat environment, the qualification score would be increased from 50 percent in the current rule, to an acceptable level of proficiency. The proposed 70 percent requirement is a commonly accepted minimum qualification score, for shotguns in the law enforcement community.
	F.5.d. Enhanced weapons.	This header would be added for formatting purposes.

Appendix B, Paragraph III.A. Each individual shall be proficient in the use of his assigned weapon(s) and shall meet prescribed standards in the following areas:	F.5.d.(1) Armed members of the security organization, assigned duties and responsibilities involving the use of any weapon or weapons not described above, shall qualify in accordance with applicable standards and scores established by a law enforcement course or an equivalent nationally recognized course for these weapons.	This new requirement would be added to account for future technological advancements in weaponry available to licensees. The phrase “national police course” would be replaced with “law enforcement course” for consistency with the terminology used nationally in reference to firearms standards and courses. Examples of “Law enforcement course or an equivalent nationally recognized course for such weapons” includes those by the Departments of Justice, Energy, or Defense.
Appendix B, Paragraph III.A. Each individual shall be proficient in the use of his assigned weapon(s) and shall meet prescribed standards in the following areas:	F.5.d.(2) Qualifying scores must be an accumulated total of 80 percent of the maximum obtainable score.	This new 80 percent qualification score requirement would be consistent and comparable with the requirements for semi-automatic rifles.
Appendix B, Paragraph IV.D. Requalification -	F.6. Requalification.	This header would be retained.

Appendix B, Paragraph IV.D. Individuals shall be weapons requalified at least every 12 months in accordance with the NRC approved licensee training and qualifications plan, and in accordance with the requirements stated in A, B, and C of this section.	F.6.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.	This requalification requirement would be retained. The phrase “every 12 months” would be replaced with the word “annually” for consistency with this proposed rule. The phrase "Individuals shall be weapons requalified" would be replaced with the phrase "Armed members of the security organization shall be re-qualified for each assigned weapon" to reflect changes in the terminology used to describe this topic. The phrase "the NRC approved licensee training and qualifications plan, and in accordance with the requirements stated in A, B, and C of this section" would be replaced with the phrase "Commission requirements and the Commission-approved training and qualification plan" to reflect changes in the terminology used to describe this topic.
Appendix B, Paragraph IV.D. Individuals shall be weapons requalified at least every 12 months in accordance with the NRC approved licensee training and qualifications plan, and in accordance with the requirements stated in A, B, and C of this section.	F.6.b. Firearms requalification must be conducted using the courses of fire outlined in Paragraph 5 of this section.	This requalification requirement would be retained. Due to changes in the threat environment, the proposed rule would specify the criteria for weapons requalification.
V. Guard, armed response personnel, and armed escort equipment.	G. Weapons, personal equipment and maintenance.	This heading would be retained and modified by adding the word “maintenance” for clarity.
	G.1. Weapons.	This header was added for formatting purposes.

Appendix B, Paragraph III.A. Each individual shall be proficient in the use of his assigned weapon(s) and shall meet prescribed standards in the following areas: 10 CFR 73.55 b.(4)(i) The licensee may not permit an individual to act as a guard, watchman armed response person, or other member of the security organization unless the individual has been trained, equipped, and qualified to perform each assigned security job duty in accordance with appendix B, in accordance with appendix B, “General Criteria for Security Personnel," to this part. Section 653 of the Energy Policy Act of 2005.	G.1.a. 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.	This new requirement would be based upon the current 10 CFR 73.55 b.(4)(i) and appendix B, Paragraph III.A. It also reflects new requirements that would implement the Energy Policy Act of 2005. This requirement would be intended to account for technological advancements in this area. Under the proposed rule, licensees could request Commission authorization to possess and use enhanced weapons that may otherwise be prohibited by individual state laws. This authority has been granted to the NRC through Section 653 of the Energy Policy Act of 2005.
	G.2. Personal equipment.	This header would be added for formatting purposes.

Appendix B, Paragraph V.A. Fixed Site--Fixed site guards and armed response personnel shall either be equipped with or have available the following security equipment appropriate to the individual's assigned contingency security related tasks or job duties as described in the licensee physical security and contingency plans:	G.2.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.	This requirement would be based upon the current appendix B, Paragraph V.A. This requirement would be intended to specify that the licensee is responsible for ensuring that each individual is provided all personal equipment required to effectively perform assigned duties and responsibilities. The phrase “has ready access to” would mean that equipment or devices, that are required to perform assigned duties, are available as described in the Commission-approved security plans, licensee
Appendix B, Paragraph V.A.5.(a) Helmet, Combat. Appendix B, Paragraph V.A.5.(b) Gas mask, full face. Appendix B, Paragraph V.A.5.(c) Body armor (bullet-resistant vest). Appendix B, Paragraph V.A.5.(d) Flashlights and batteries. Appendix B, Paragraph V.A.5.(e) Baton. Appendix B, Paragraph V.A.5.(f) Handcuffs. Appendix B, Paragraph V.A.5.(g)	G.2.b. The licensee shall provide armed security personnel, 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) Duress alarms. (5) Two-way portable radios (handi-talkie) 2 channels minimum, 1 operating and 1 emergency.	This requirement combines the current requirements appendix B, Paragraph V.A.5(b), 5(c), 5(g), 9, and 10. Due to changes in the threat environment, the NRC has determined that this list of equipment would be the minimum required to effectively perform response duties.

Ammunition-equipment belt. Appendix B, Paragraph V.A.6. Binoculars. Appendix B, Paragraph V.A.7. Night vision aids, i.e., hand-fired illumination flares or equivalent. Appendix B, Paragraph V.A.8. Tear gas or other nonlethal gas. Appendix B, Paragraph V.A.9. Duress alarms. Appendix B, Paragraph V.A.10. Two-way portable radios (handi-talkie) 2 channels minimum, 1 operating and 1 emergency.		
Appendix B, Paragraph V.A.5.(a) Helmet, Combat. Appendix B, Paragraph V.A.5.(b) Gas mask, full face. Appendix B, Paragraph V.A.5.(c) Body armor (bullet-resistant vest). Appendix B, Paragraph V.A.5.(d) Flashlights and batteries. Appendix B, Paragraph V.A.5.(e) Baton. Appendix B, Paragraph V.A.5.(f) Handcuffs. Appendix B, Paragraph V.A.5.(g)	G.2.c. Based upon the licensee protective strategy and the specific duties and responsibilities assigned to each individual, the licensee should provide, 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	This requirement would be based upon the current appendix B, Paragraph V.A.5. The NRC has determined that this list of additional equipment must be provided because such equipment is required to effectively implement the licensee protective strategy and the specific duties and responsibilities assigned to each individual. The current requirement appendix B, Paragraph V.A.5.(a) "Helmet, combat" would be deleted because the NRC has determined that although the use of this item is

Ammunition-equipment belt. Appendix B, Paragraph V.A.6 Binoculars. Appendix B, Paragraph V.A.7. Night vision aids, i.e., hand-fired illumination flares or equivalent. Appendix B, Paragraph V.A.8. Tear gas or other nonlethal gas. Appendix B, Paragraph V.A.9. Duress alarms. Appendix B, Paragraph V.A.10. Two-way portable radios (handi-talkie) 2 channels minimum, 1 operating and 1 emergency.	equivalent. (7) Tear gas or other non-lethal gas.	recommended it is an optional item that is not required to effectively implement a protective strategy or perform assigned duties and responsibilities. The proposed addition in (2) " ... or other non-lethal weapons" would recognize that the use of batons and other non-lethal weapons by armed security officers is subject to state law. Related to the use of non-lethal weapons, each state has minimum training requirements for armed private security officers.
	G.3. Maintenance.	This heading would be added for formatting purposes.
Appendix B, Paragraph III.A. Each individual shall be proficient in the use of his assigned weapon(s) and shall meet prescribed standards in the following areas:	G.3.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.	This requirement would be based upon the current appendix B, Paragraph III.A. This proposed rule would require a firearms maintenance program to ensure weapons and ammunition are properly maintained, function as designed, and are properly stored and accounted for. In order to certify armorer, each weapon manufacturer provides training regarding the maintenance, care and repair of weapons they provide to licensees. The Commission believes that armorers must be certified to ensure that the quality of maintenance, care and repair of the weapons are in accordance with manufacturers specifications.

	H. Records.	This heading would be added formatting purposes.
Appendix B, Paragraph II.A. The licensee or the agent shall maintain documentation of the current plan and retain this documentation of the plan as a record for three years after the close of period for which the licensee possesses the special nuclear material under each license for which the plan was developed and, if any portion of the plan is superseded, retain the material that is superseded for three years after each change.	H.1. The licensee shall retain all reports, records, or other documentation required by this appendix in accordance with the requirements of § 73.55(r).	This requirement would be added to replace the current appendix B, Paragraph II.A, for consistency with the proposed § 73.55(r), and to specify the records retention requirement. This requirement would be intended to consolidate all records retention requirements.

Appendix B, Paragraph I.C. The physical fitness qualification of each guard, armed response person, armed escort, and other security force member shall be documented... Appendix B, Paragraph I.C. The licensee shall retain this documentation as a record for three years from the date of each qualification. Appendix B, Paragraph I.E. The licensee shall document each individual's physical requalification and shall retain this documentation of requalification as a record for three years from the date of each requalification. Appendix B, Paragraph II.B. The qualifications of each individual must be documented... Appendix B, Paragraph II.B. The licensee shall retain this documentation of each individual's qualifications as a record for three years after the employee ends employment in the security-related capacity and for three years after the close of period for which the licensee possesses the special nuclear material under each license, and superseded material for three years after each change.	H.2. The licensee shall retain each individual's initial qualification record for three (3) years after termination of the individual's employment and shall retain each re-qualification record for three (3) years after it is superceded.	This requirement would combine all record retention requirements currently in appendix B.

Appendix B, Paragraph II.E. The results of requalification must be documented... Appendix B, Paragraph II.E. The licensee shall retain this documentation of each individual's requalification as a record for three years from the date of each requalification. Appendix B, Paragraph IV. The results of weapons qualification and requalification must be documented by requalification must be documented by the licensee or the licensee's agent. Appendix B, Paragraph IV. The licensee shall retain this documentation of each qualification as a record for three years from the date of the qualification or requalification, as appropriate.		
Appendix B, Paragraph I.F. The results of suitability, physical, and mental qualifications data and test results must be documented by the licensee or the licensee's agent. The licensee or the agent shall retain this documentation as a record for three years from the date of obtaining and recording these results.	H.3. The licensee shall document data and test results from each individual's suitability, physical, and psychological qualification and shall retain this documentation as a record for three years from the date of obtaining and recording these results.	This requirement would combine two requirements currently in appendix B.
	I. Audits and reviews.	This heading would be added to ensure consistency with the structure of the appendix.
	The licensee shall review the Commission-approved training and qualification plan in accordance with the requirements of § 73.55(n).	This requirement would be added for consistency with audit and review requirements of the proposed 10 CFR 73.55(n).

Definitions	J. Definitions	This heading would be brought forward from the current rule and would be renumbered accordingly.
Terms defined in Parts 50, 70, and 73 of this chapter have the same meaning when used in this appendix.	Terms defined in Parts 50, 70, and 73 of this chapter have the same meaning when used in this appendix.	This requirement would be brought forward from the current rule and would be renumbered accordingly.

Table 7 - Part 73 Appendix C Section II
Nuclear Power Plants Safeguards Contingency Plans

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
Appendix C	Section II: Nuclear power plant safeguards contingency plans.	This paragraph and header would be added to independently address Nuclear Power Reactor Safeguards Contingency Plan requirements without impacting other licensees. The proposed requirements addressed in this proposed paragraph retain and incorporate the requirements of the appendix C.
Introduction	(a) Introduction	This requirement would be retained.
	The safeguards contingency plan must describe how the criteria set forth in this appendix will be satisfied through implementation and must provide specific goals, objectives and general guidance to licensee personnel to facilitate the initiation and completion of predetermined and exercised responses to threats, up to and including the design basis threat described in § 73.1(a)(1).	This requirement would be added to generally describe the Commission's expectations for the content of the safeguards contingency plan.
Contents of the Plan	Contents of the plan.	This requirement would be retained.

Each licensee safeguards contingency plan shall include five categories of information: 1. Background 2. Generic Planning Base 3. Licensee Planning Base 4. Responsibility Matrix 5. Procedures	(b) Each safeguards contingency plan must include the following twelve (12) categories of information: (1) Background. (2) Generic Planning Base. (3) Licensee Planning Base. (4) Responsibility Matrix. (5) Primary Security Functions. (6) Response Capabilities. (7) Protective Strategy. (8) Integrated Response Plan. (9) Threat Warning System. (10) Performance Evaluation Program. (11) Audits and Reviews. (12) Implementing Procedures.	This requirement would be retained with editorial changes. The current categories of information (1) through (5) would be retained with (5) being reformatted to (12) and renamed "Implementing Procedures" to update the terminology used to identify this category of information. The proposed categories of information (5) through (11) would be added to improve the usefulness and applicability of the safeguards contingency plan.
1. Background.	(c) Background.	This header would be retained with editorial change.
Under the following topics, this category of information shall identify and define the perceived dangers and incidents with which the plan will deal and the general way it will handle these:	(c)(1) Consistent with the design basis threat specified in section § 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.	This requirement would be retained with information added to identify specific goals, objectives and general information for the development of the safeguards contingency plan.

1.b. Purpose of the Plan -- A discussion of the general aims and operational concepts underlying implementation of the plan. Introduction: The goals of licensee safeguards contingency plans for responding to threats, thefts, and radiological sabotage are:	(c)(2) Licensees shall describe the general goals and operational concepts underlying implementation of the approved safeguards contingency plan, to include, but not limited to the following:	This requirement would be retained with editorial changes. The header “Purpose of the Plan” would be deleted because purpose is described in the proposed paragraph (a)(2). The phrase “A discussion of the general aims and” would be deleted because the specific goals and objectives discussed in the proposed paragraph c)(1) would include "general aims", therefore, it is not necessary to further break this topic area into individual components. The phrase ",to include, but not limited to the following" would be added to provide flexibility for the licensee to add information not specifically listed.
1.c. Scope of the Plan -- A delineation of the types of incidents covered in the plan.	(c)(2)(I) The types of incidents covered.	This requirement would be retained with editorial changes. The header “Scope of the Plan” would be deleted because the scope of the safeguards contingency plan under this proposed rule would not be limited to only a delineation of the types of incidents covered in the plan.
Introduction: A licensee safeguards contingency plan is a documented plan to give guidance to licensee personnel in order to accomplish specific defined objectives...	(c)(2)(ii) The specific goals and objectives to be accomplished.	This requirement would be retained with additional information added for the identification of specific goals and objectives to be accomplished to ensure the plan is appropriately oriented toward mission accomplishment.

Background: Under the following topics, this category of information shall identify and define the perceived dangers and incidents with which the plan will deal and the general way it will handle these:	(c)(2)(iii) The different elements of the onsite physical protection program that are used to provide at all times the capability to detect, assess, intercept, challenge, delay, and neutralize threats, up to and including the design basis threat relative to the perceived dangers and incidents described in the Commission-approved safeguards contingency plan.	This requirement would be retained with additional information added to describe defense-in-depth concepts as they apply at each site and how the individual components that make up the onsite physical protection program would work together to ensure the capability to detect, assess, intercept, challenge, delay, and neutralize the threats are consistent with the proposed requirements of § 73.55.
Introduction: The goals of licensee safeguards contingency plans...are: (1) to organize the response effort at the licensee level,	(c)(2)(iv) How the onsite response effort is organized and coordinated to ensure that licensees capability to prevent significant core damage and spent fuel sabotage is maintained throughout each type of incident covered.	This requirement would be retained with additional information added to describe the elements of a site integrated response to prevent significant core damage and spent fuel sabotage.
Introduction: The goals of licensee safeguards contingency plans...are: (3) to ensure the integration of the licensee response with the responses by other entities, and; Introduction: It is important to note that a licensee's safeguards contingency plan is intended to be complimentary to any emergency plans developed pursuant to appendix E to part 50 or to § 70.22(I) of this chapter.	(c)(2)(v) How the onsite response effort is integrated to include specific procedures, guidance, and strategies to maintain or restore core cooling, containment, and spent fuel pool cooling capabilities using existing or readily available resources (equipment and personnel) that can be effectively implemented under the circumstances associated with loss of large areas of the plant due to explosions or fires.	This requirement would be retained with additional information provided for an integrated response as addressed in the proposed paragraph (j). Reference to appendix E to part 50 or to § 70.22(I) would no longer be required because the performance standard for this proposed requirement would be broad enough to include these references and any other emergency plans developed as a result of Commission mandated enhancements.

1.d. Definitions -- A list of terms and their definitions used in describing operational and technical aspects of the plan.	(c)(2)(vi) A list of terms and their definitions used in describing operational and technical aspects of the approved safeguards contingency plan.	This requirement would be retained with editorial changes. The header "Definitions" is deleted because it would no longer be required under the new format of this proposed rule. The phrase "approved safeguards contingency" would be added to reflect changes to the terminology used to describe this topic.
2. Generic Planning Base.	(d) Generic planning base.	This requirement would be retained.
2. Under the following topics, this category of information shall define the criteria for initiation and termination of responses to safeguards contingencies together with the specific decisions, actions, and supporting information needed to bring about such responses:	(d)(1) Licensees shall define the criteria for initiation and termination of responses to threats to include the specific decisions, actions, and supporting information needed to respond to each type of incident covered by the approved safeguards contingency plan.	This requirement would be retained with editorial changes. The phrase "Under the following topics" would be replaced with the phrase "The licensee shall define" to establish the required action to be taken by the licensee. The phrase "safeguards contingencies" would be replaced by the word "threats" to reflect changes in the terminology used to describe this topic. The phrase "together with" would be replaced with the phrase "to include". The phrase "bring about such responses" is replaced by the phrase "respond to each type of incident covered by the approved safeguards contingency plan."

2.a. Such events may include alarms or other indications signaling penetration of a protected area, vital area, or material access area; material control or material accounting indications of material missing or unaccounted for; or threat indications--either verbal, such as telephoned threats, or implied, such as escalating civil disturbances.	(d)(2) Licensees shall ensure early detection of unauthorized activities and shall respond to all alarms or other indications of a threat condition such as, tampering, bomb threats, unauthorized barrier penetration (vehicle or personnel), missing or unaccounted for nuclear material, escalating civil disturbances, imminent threat notification, or other threat warnings.	This requirement would be retained with editorial changes. Reference to specific site areas would be deleted. The licensee would be required to respond to unauthorized activities where detection has occurred. Examples provided would be revised for consistency with the terminology used in the proposed rule and would not be intended to be all inclusive.
Appendix C - Introduction. An acceptable safeguards contingency plan must contain:	(d)(3) The safeguards contingency plan must:	This requirement would be retained with editorial changes. The phrase "an acceptable" is deleted because the requirements of this proposed rule address what would be acceptable.
2.a. Identification of those events that will be used for signaling the beginning or aggravation of a safeguards contingency according to how they are perceived initially by licensee's personnel.	(d)(3)(i) Identify the types of events that signal the beginning or initiation of a safeguards contingency event.	This requirement would be retained with editorial changes. The phrase “according to how they are perceived initially by licensee's personnel” would be deleted because the concept of perceived is captured through assessment.
Introduction: The goals of licensee safeguards contingency plans...are: (2) to provide predetermined, structured responses by licensees to safeguards contingencies,	(d)(3)(ii) Provide predetermined and structured responses to each type of postulated event.	This requirement would be retained with editorial changes. The phrase “safeguards contingencies” has been replaced with “each type of postulated event” to include a wider range of potential events.

2.b. Definition of the specific objective to be accomplished relative to each identified event.	(d)(3)(iii) Define specific goals and objectives for response to each postulated event.	This requirement would be retained with editorial changes. The word "goals" would be added for consistency with the proposed Paragraph (a)(3).
2.b.(1) a predetermined set of decisions and actions to satisfy stated objectives,	(d)(3)(iv) Identify the predetermined decisions and actions which are required to satisfy the written goals and objectives for each postulated event.	This requirement would be retained with more specific information being provided to ensure that written goals and objectives are identified for each postulated event.
2.b.(2) an identification of the data, criteria, procedures, and mechanisms necessary to efficiently implement the decisions, and;	(d)(3)(v) Identify the data, criteria, procedures, mechanisms and logistical support necessary to implement the predetermined decisions and actions.	This requirement would be retained with editorial changes. The word "efficiently" would be deleted because it is considered to be an arbitrary term that would not describe the performance standard of this proposed requirement.
2.b.(3) a stipulation of the individual, group, or organizational entity responsible for each decision and action.	(d)(3)(vi) Identify the individuals, groups, or organizational entities responsible for each predetermined decision and action.	This requirement would be retained with editorial changes. The use of the word “predetermined” has been inserted to organizationally align decisions and actions to responsible entities.
2.b.(3) a stipulation of the individual, group, or organizational entity responsible for each decision and action.	(d)(3)(vii) Define the command-and-control structure required to coordinate each individual, group, or organizational entity carrying out predetermined actions.	This requirement would be retained with editorial changes. The required elements of command and control have been added to establish clear lines of authority.

Introduction: The goals of licensee safeguards contingency plans...are: (4) to achieve a measurable performance in response capability.	(d)(3)(viii) Describe how effectiveness will be measured and demonstrated to include the effectiveness of the capability to detect, assess, intercept, challenge, delay, and neutralize threats, up to and including the design basis threat.	This requirement has been retained with editorial changes. A change has been made to replace the word "response" with the phrase "detect, assess, intercept, challenge, delay, and neutralize" to provide a more detailed description of system effectiveness.
3. Licensee Planning Base.	(e) Licensee planning base.	This requirement would be retained.
This category of information shall include the factors affecting contingency planning that are specific for each facility or means of transportation. 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. The following topics should be addressed:	(e) Licensees shall describe the site-specific factors affecting contingency planning and shall develop plans for actions to be taken in response to postulated threats. The following topics must be addressed:	This requirement would be retained with editorial changes. The phrase “or means of transportation” is deleted because this phrase does not apply to nuclear power reactor licensees. The phrase "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.
3.a. Licensee's Organizational Structure for Contingency Responses. A delineation of the organization's chain of command and delegation of authority as these apply to safeguards contingencies.	(e)(1) Organizational Structure. The safeguards contingency plan must describe the organization's chain of command and delegation of authority during safeguards contingencies, to include a description of how command-and-control functions will be coordinated and maintained.	This requirement has been retained with more detailed information being provided for the integration of command groups, succession of command, and control functions.
3.b. Physical Layout.	(e)(2) Physical layout.	This requirement would be retained.

3.b.(i) Fixed Sites. A description of the physical structures and their location on the site...	(e)(2)(i) The safeguards contingency plan must include a site description, to include maps and drawings, of the physical structures and their locations.	This requirement would be retained with editorial changes. The header “Fixed Sites” would be deleted because it would not be necessary for the purpose of this proposed rule. Specific information to permit orientation and familiarization of the site would also be included.
3.b.(i) A description...and a description of the site in relation to nearby town, roads, and other environmental features important to the effective coordination of response operations.	(e)(2)(i)(A) Site Description. The site description must address the site location in relation to nearby towns, transportation routes (e.g., rail, water, air, roads), pipelines, hazardous material facilities, onsite independent spent fuel storage installations, and pertinent environmental features that may have an effect upon coordination of response operations.	This requirement has been retained with more detailed information being included to consider the sites geographic relationship to the community and environment.
3.b.(i) Particular emphasis should be placed on main and alternate entry routes for law-enforcement assistance forces and the location of control points for marshaling and coordinating response activities.	(e)(2)(i)(B) Approaches. Particular emphasis must be placed on main and alternate entry routes for law-enforcement or other offsite support agencies and the location of control points for marshaling and coordinating response activities.	This requirement would be retained with editorial changes. The word "should" has been replaced with the word "must" to establish this language as a requirement.
	(e)(2)(ii) Licensees with co-located Independent Spent Fuel Storage Installations shall describe response procedures for both the operating reactor and the Independent Spent Fuel Storage Installation to include how onsite and offsite responders will be coordinated and used for incidents occurring outside the protected area.	This requirement would be retained with more detailed information being provided for response to incidents occurring outside the protected area and for the utilization of assets.

3.c. Safeguards Systems Hardware. A description of the physical security and accounting system hardware that influence how the licensee will respond to an event. Examples of systems to be discussed are communications, alarms, locks, seals, area access, armaments, and surveillance.	(e)(3) Safeguards Systems Hardware. The safeguards contingency plan must contain a description of the physical security and material accounting system hardware that influence how the licensee will respond to an event.	This requirement would be retained with editorial changes to specify hardware for material accountability.
3.d. Law Enforcement Assistance.	(e)(4) Law enforcement assistance.	This requirement would be retained.
3.d. A listing of available local law enforcement agencies and a description of their response capabilities and their criteria for response; and...	(e)(4)(i) The safeguards contingency plan must contain a listing of available local, state, and Federal law enforcement agencies and a general description of response capabilities, to include number of personnel, types of weapons, and estimated response time lines.	This requirement would be retained with more detailed information being provided for documenting supporting agency capabilities and assets.
3.d. ...and a discussion of working agreements or arrangements for communicating with these agencies.	(e)(4)(ii) The safeguards contingency plan must contain a discussion of working agreements with offsite law enforcement agencies to include criteria for response, command and control protocols, and communication procedures.	This requirement would be retained with the addition of written information to be included in working agreements with offsite law enforcement agencies.

3.e. Policy Constraints and Assumptions. A discussion of State laws, local ordinances, and company policies and practices that govern licensee response to incidents. Examples that may be discussed include: (1) Use of deadly force; (2) Use of employee property; (3) Use of off-duty employees; (4) Site security jurisdictional boundaries.	(e)(5) Policy constraints and assumptions. The safeguards contingency plan must 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.	This requirement would be retained. The text of 3.e.(2) "Use of Employee property" would be deleted because this information would not be considered relevant for discussion under policy constraints and assumptions. The requirement would be added to implement applicable provisions from the EPAct of 2005. This requirement is not applicable to licensees that possess such weaponry under authority separate from EPAct 2005.
3.f. Administrative and Logistical Considerations --	(e)(6) Administrative and logistical considerations.	This requirement would be retained.
3.f. Descriptions of licensee practices that may have an influence on the response to safeguards contingency events. The considerations shall include a description of the procedures that will be used for ensuring that all equipment needed to effect a successful response to a safeguards contingency will be easily accessible, in good working order, and in sufficient supply to provide redundancy in case of equipment failure.	(e)(6)(i) The safeguards contingency plan must contain a description of licensee practices which influence how the licensee responds to a threat to include, but not limited to, a description of the procedures that will be used for ensuring that all equipment needed to effect a successful response will be readily accessible, in good working order, and in sufficient supply to provide redundancy in case of equipment failure.	This requirement would be retained with information added to reflect changes in the terminology used to describe this topic.
4. Responsibility Matrix.	(f) Responsibility matrix.	This requirement would be retained.

This category of information consists of detailed identification of the organizational entities responsible for each decision and action associated with specific responses to safeguards contingencies.	(f)(1) The safeguards contingency plan must describe the organizational entities that are responsible for each decision and action associated with responses to threats.	This requirement would be retained with information added to reflect changes in the terminology used to describe this topic.
For each initiating event, a tabulation shall be made for each response entity depicting the assignment of responsibilities for all decisions and actions to be taken in response to the initiating event. (Not all entities will have assigned responsibilities for any given initiating event.)	(f)(1)(i) For each identified initiating event, a tabulation must be made for each response depicting the assignment of responsibilities for all decisions and actions to be taken.	This requirement would be retained with editorial changes. The parenthetical phrase "(Not all entities will have assigned responsibilities for any given initiating event)" would be deleted because it is considered to be constricting information.
The tabulations in the Responsibility Matrix shall provide an overall picture of the response actions and their interrelationships.	(f)(1)(ii) The tabulations described in the responsibility matrix must provide an overall description of response actions and interrelationships.	This requirement would be retained with editorial changes. The word “shall” has been replaced with “must” to establish this language as a requirement.
Safeguards responsibilities shall be assigned in a manner that precludes conflict in duties or responsibilities that would prevent the execution of the plan in any safeguards contingency.	(f)(2) Licensees shall ensure that duties and responsibilities required by the approved safeguards contingency plan do not conflict with or prevent the execution of other site emergency plans.	This requirement would be retained with editorial changes.
Safeguards responsibilities shall be assigned in a manner that precludes conflict in duties or responsibilities that would prevent the execution of the plan in any safeguards contingency.	(f)(3) Licensees shall identify and discuss potential areas of conflict between site plans in the integrated response plan required by Section II(b)(8) of this appendix.	This requirement would be retained with added written discussion (text) in the plan to document consideration of other plans to preclude conflict between multiple plans.

	(f)(4) Licensees shall address safety/security interface issues in accordance with the requirements of § 73.58 to ensure activities by the security organization, maintenance, operations, and other onsite entities are coordinated in a manner that precludes conflict during both normal and emergency conditions.	This requirement would be added to address communication between licensee safety and security entities, to ensure that activities involving one organizational entity do not adversely affect another. Details would be addressed in the proposed § 73.58 safety/security interface.
	(g) Primary security functions.	This requirement would be added to improve the usefulness and applicability of the safeguards contingency plan.
73.55(h)(4)(iii)(A) Requiring responding guards or other armed response personnel to interpose themselves between vital areas and material access areas and any adversary attempting entry for the purpose of radiological sabotage or theft of special nuclear material and to intercept any person exiting with special nuclear material, and,...	(g)(1) Licensees shall establish and maintain at all times, the capability to detect, assess, and respond to all threats to the facility up to and including the design basis threat.	This requirement would be retained with editorial changes. The phrase "radiological sabotage" is replaced with the phrase "all threats up to and including the design basis threat" to more accurately represent the standard that the licensee also protect against perceived threats not contained in the design basis threat.
73.55(h)(6) To facilitate initial response to detection of penetration of the protected area and assessment of the existence of a threat, a capability of observing the isolation zones and the physical barrier at the perimeter of the protected area shall be provided, preferably by means of closed circuit television or by other suitable means which limit exposure of responding personnel to possible attack.	(g)(2) To facilitate initial response to a threat, licensees shall ensure the capability to observe all areas of the facility in a manner that ensures early detection of unauthorized activities and limits exposure of responding personnel to possible attack.	This requirement would be retained with editorial changes. Early detection has been added to permit a timely and effective response. The goal is to observe and detect potential threats as far from the facility as possible.

	(g)(3) Licensees shall generally describe how the primary security functions are integrated to provide defense-in-depth and are maintained despite the loss of any single element of the onsite physical protection program.	This requirement would be added to describe the concept of defense-in-depth for improved system effectiveness.
	(g)(4) Licensees description must begin with onsite physical protection measures implemented in the outermost facility perimeter, and must move inward through those measures implemented to protect vital and target set equipment.	This requirement would be added to further describe the concept of defense-in-depth for improved system effectiveness.
	(h) Response capabilities.	This requirement would be added.
73.55(h)(4)(iii)(A) Requiring responding guards or other armed response personnel to interpose themselves between vital areas and material access areas and any adversary attempting entry for the purpose of radiological sabotage or theft of special nuclear material and to intercept any person exiting with special nuclear material, and,..	(h)(1) Licensees shall establish and maintain at all times the capability to intercept, challenge, delay, and neutralize threats up to and up to and including the design basis threat.	This requirement would be retained with editorial changes. The phrase "radiological sabotage" is replaced with the phrase "all threats up to and including the design basis threat" for consistency with the proposed § 73.55.
Appendix C, Paragraph 4. For each initiating event, a tabulation shall be made for each response entity depicting the assignment of responsibilities for all decisions and actions to be taken in response to the initiating event.	(h)(2) Licensees shall identify the personnel, equipment, and resources necessary to perform the actions required to prevent significant core damage and spent fuel sabotage in response to postulated events.	The requirement would be retained with information added to identify the allocation of personnel and the availability of assets required to be implemented in response to postulated events.

	(h)(3) Licensees shall ensure that predetermined actions can be completed under the postulated conditions.	This requirement would be added. The word “predetermined” is used to provide for the accomplishment of automatic actions to achieve the security mission.
§ 73.55(h)(3) The total number of guards, and armed, trained personnel immediately available at the facility to fulfill these response requirements shall nominally be ten (10), unless specifically required otherwise on a case by case basis by the Commission; however, this number may not be reduced to less than five (5) guards.	(h)(4) Licensees shall provide at all times an armed response team comprised of trained and qualified personnel who possess the knowledge, skills, abilities, and equipment required to implement the Commission-approved safeguards contingency plan and site protective strategy. The plan must include a description of the armed response team including the following:	This requirement would be retained with editorial changes. The requirement would be based on § 73.55(h)(3) and would describe the performance standard for personnel assigned armed response duties.
§ 73.55(h)(3) The total number of guards, and armed, trained personnel immediately available at the facility to fulfill these response requirements shall nominally be ten (10), unless specifically required otherwise on a case by case basis by the Commission; however, this number may not be reduced to less than five (5) guards.	(h)(4)(i) The authorized minimum number of armed responders, available at all times inside the protected area.	This requirement would be retained with information added to establish the number of personnel required to be assigned armed response duties within the protected area. This is intended to ensure that predetermined positions documented in approved contingency plans and are occupied during threat situations.
§ 73.55(h)(3) The total number of guards, and armed, trained personnel immediately available at the facility to fulfill these response requirements shall nominally be ten (10), unless specifically required otherwise on a case by case basis by the Commission; however, this number may not be reduced to less than five (5) guards.	(h)(4)(ii) The authorized minimum number of armed security officers, available onsite at all times.	This requirement would be retained with information added to establish the number of personnel required to be assigned armed response duties on site. This is intended to ensure that predetermined positions documented in approved contingency plans and are occupied during threat situations.

	(h)(5) The total number of armed responders and armed security officers must be documented in the approved security plans and documented as a component of the protective strategy.	This requirement would be added to document the number of armed response personnel and their roles and relationships to the protective strategy.
	(h)(6) Licensees shall ensure that individuals assigned duties and responsibilities to implement the Safeguards Contingency Plan are trained and qualified in accordance with appendix B of this part and the Commission-approved security plans.	This requirement would be added to ensure assigned personnel are trained to perform their assigned duties and responsibilities.
	(i) Protective strategy.	This header is added for formatting purposes.
	(i)(1) Licensees shall develop, maintain, and implement a written protective strategy that describes the deployment of the armed response team relative to the general goals, operational concepts, performance objectives, and specific actions to be accomplished by each individual in response to postulated events.	This requirement would be added to provide tactical planning information for the armed response team and each individual in response to threats.
	(i)(2) The protective strategy must:	This header is added for formatting purposes.

§73.55(h)(4)(iii)(A) Requiring responding guards or other armed response personnel to interpose themselves between vital areas and material access areas and any adversary attempting entry for the purpose of radiological sabotage or theft of special nuclear material and to intercept any person exiting with special nuclear material, and,	(i)(2)(i) Be designed to prevent significant core damage and spent fuel sabotage through the coordinated implementation of specific actions and strategies required to intercept, challenge, delay, and neutralize threats up to and including the design basis threat of radiological sabotage.	This requirement would be retained and revised to describe the design of the licensee protective strategy consistent with the proposed § 73.55(b)(2). Most significantly, the word “interpose” would be replaced by the phrase “intercept, challenge, delay, and neutralize” to provide a measurable performance based requirement that identifies the specific actions required to satisfy the action "interpose" as required by the current § 73.55(h)(4)(iii)(A), and to provide a measurable performance based requirement against which the effectiveness of the licensee protective strategy could be measured.
	(i)(2)(ii) Describe and consider site specific conditions, to include but not limited to, facility layout, the location of target set equipment and elements, target set equipment that is in maintenance or out of service, and the potential effects that unauthorized electronic access to safety and security systems may have on the protective strategy capability to prevent significant core damage and spent fuel sabotage.	This requirement would be added based on changes to the threat environment the Commission has determined that it is necessary to emphasize consideration of the listed areas for design and planning purposes.
	(i)(2)(iii) Identify predetermined actions and time lines for the deployment of armed personnel.	This requirement would be added to identify “predetermined actions” to provide for automatic actions toward accomplishing the security mission.

	(i)(2)(iv) Provide bullet resisting protected positions with appropriate fields of fire.	This requirement would be added to provide a performance based requirement for the placement/location of Bullet-Resisting Enclosures (BREs). This proposed requirement would ensure that each position would be of sufficient strength to enhance survivability of armed personnel against the design basis threat and would ensure that assigned areas of responsibility are clearly visible and within the functional capability of assigned weapons.
§ 73.55(h)(6) To facilitate initial response to detection of penetration ...which limit exposure of responding personnel to possible attack.	(i)(2)(v) Limit exposure of security personnel to possible attack.	This requirement would be retained with editorial changes added to describe the ballistic protection or use of available cover and concealment for security personnel.
§73.55(f)(1) Each guard, watchman or armed response individual on duty shall be capable of maintaining continuous communication with an individual in each continuously manned alarm station required by paragraph (e)(1) of this section, who shall be capable of calling for assistance from other guards, watchmen, and armed response personnel and from local law enforcement authorities.	(i)(3) Licensees shall 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 and that facilitates response in accordance with the integrated response plan.	This requirement would be retained with editorial changes added to describe the elements of integrated incident command during postulated events.
	(j) Integrated Response Plan	This new header would be added for formatting purposes.

Introduction: It is important to note that a licensee's safeguards contingency plan is intended to be complimentary to any emergency plans developed pursuant to appendix E to part 50 or to § 70.22(i) of this chapter.	(j)(1) Licensees shall document, maintain, and implement an Integrated Response Plan which must identify, describe, and coordinate actions to be taken by licensee personnel and offsite agencies during a contingency event or other emergency situation.	This requirement would be retained with editorial changes. The requirement would describe integrated and coordinated responses to threats.
	(j)(2) The Integrated Response Plan must:	This requirement would be added to improve the usefulness and applicability of the safeguards contingency plan.
	(j)(2)(i) Be designed to integrate and coordinate all actions to be taken in response to an emergency event in a manner that will ensure that each site plan and procedure can be successfully implemented without conflict from other plans and procedures.	This requirement would be added to ensure the design of an integrated response plan that has been developed in coordination and conjunction with other plans.
	(j)(2)(ii) Include specific procedures, guidance, and strategies to maintain or restore core cooling, containment, and spent fuel pool cooling capabilities using existing or readily available resources (equipment and personnel) that can be effectively implemented under the circumstances associated with loss of large areas of the plant due to explosions or fires.	This requirement would be added to ensure the design of an integrated response plan that addresses a myriad of postulated events within the design basis threat environment and to develop mitigating strategies for events that may exceed the design basis threat.

	(j)(2)(iii) Ensure that onsite staffing levels, facilities, and equipment required for response to any identified event, are readily available and capable of fulfilling their intended purpose.	This requirement would be added to describe the availability of systems and assets to ensure a high state of readiness is maintained for postulated events.
	(j)(2)(iv) Provide emergency action levels to ensure that threats result in at least a notification of unusual event and implement procedures for the assignment of a predetermined classification to specific events.	This requirement would be added to ensure that event information is communicated in a timely and accurate manner.
	(j)(2)(v) Include specific procedures, guidance, and strategies describing cyber incident response and recovery.	This requirement would be added to consider advanced threats related to computer technology.
	(j)(3) Licensees shall:	This new header is added for formatting purposes.
	(j)(3)(i) Reconfirm on an annual basis, liaison with local, state, and Federal law enforcement agencies, established in accordance with § 73.55(k)(8), to include communication protocols, command and control structure, marshaling locations, estimated response times, and anticipated response capabilities and specialized equipment.	This requirement would be added to establish a periodic standard for maintaining liaison with off-site law enforcement resources to ensure a continual and ongoing understanding of all aspects of a response to potential threats.

	(j)(3)(ii) Provide required training to include simulator training for the operations response to security events (e.g. loss of ultimate heat sink) for nuclear power reactor personnel in accordance with site procedures to ensure the operational readiness of personnel commensurate with assigned duties and responsibilities.	This requirement would be added to provide for training of personnel to ensure they possess the knowledge, skills, and abilities required to perform assigned duties and responsibilities.
	(j)(3)(iii) Periodically train personnel in accordance with site procedures to respond to a hostage or duress situation.	This requirement would be added to provide training of personnel to ensure they possess the tactical and negotiations skills, knowledge and abilities needed to respond to a hostage or duress situation.
	(j)(3)(iv) Determine the possible effects that nearby hazardous material facilities may have upon site response plans and modify response plans, procedures, and equipment as necessary.	This requirement would be added to provide for the identification of site specific operational conditions that may effect how the licensee responds to threats.
	(j)(3)(v) Ensure that identified actions are achievable under postulated conditions.	This requirement would be added to ensure that actions identified in the safeguards contingency plan, protective strategy, integrated response plan, and any other emergency plans, are achievable under postulated conditions.
	(k) Threat warning system.	This new header is added for formatting purposes.

	(k)(1) Licensees shall implement a "Threat warning system" which identifies specific graduated protective measures and actions to be taken to increase licensee preparedness against a heightened or imminent threat of attack.	This requirement would be added to provide for progressive steps to gradually enhance security based on perceived or identified threat.
	(k)(2) Licensees shall ensure that the specific protective measures and actions identified for each threat level are consistent with the Commission-approved safeguards contingency plan, and other site security, and emergency plans and procedures.	This requirement would be added to ensure preplanned actions (protective measures) are consistent with other plans. The Commission has determined that because of changes to the threat environment this proposed requirement would be needed to emphasize the importance of coordinating all site plans in a manner that precludes conflict.
	(k)(3) Upon notification by an authorized representative of the Commission, licensees shall implement the specific protective measures assigned to the threat level indicated by the Commission representative.	This requirement would be added to provide for the implementation of preplanned actions in response to specific threat levels or conditions.
	(l) Performance Evaluation Program	This new header would be added for formatting purposes.

	(l)(1) Licensees shall document and maintain a Performance Evaluation Program that describes how the licensee will demonstrate and assess the effectiveness of the onsite physical protection program to prevent significant core damage and spent fuel sabotage, and to include the capability of armed personnel to carry out their assigned duties and responsibilities.	This requirement would be added to ensure that the licensee maintains a Performance Evaluation Plan to test, evaluate, determine and improve upon the effectiveness of onsite physical protection program to protect the identified targets and target sets in accordance with the security mission.
	(l)(2) The Performance Evaluation Program must include procedures for the conduct of quarterly drills and annual force-on-force exercises that are designed to demonstrate the effectiveness of the licensee's capability to detect, assess, intercept, challenge, delay, and neutralize a simulated threat.	This requirement would be added to establish procedures and frequencies for the conduct of drills and exercises to ensure that system effectiveness determinations are made.
	(l)(2)(i) The scope of drills conducted for training purposes must be determined by the licensee as needed, and can be limited to specific portions of the site protective strategy.	This requirement would be added to provide for the conduct of drills for training purposes only.
	(l)(2)(ii) Drills, exercises, and other training must be conducted under conditions that simulate as closely as practical the site specific conditions under which each member will, or may be, required to perform assigned duties and responsibilities.	This requirement would be added to ensure drills and exercises are realistic in that they simulate as closely as possible, the physical conditions (running, lifting, climbing) and mental stress levels (decision making, radio communications, strategy changes) that will be experienced in an actual event.

	(l)(2)(iii) Licensees shall document each performance evaluation to include, but not limited to, scenarios, participants, and critiques.	This requirement would be added to ensure that comprehensive records are maintained.
	(l)(2)(iv) Each drill and exercise must include a documented post exercise critique in which participants identify failures, deficiencies, or other findings in performance, plans, equipment, or strategies.	This requirement would be added to ensure that comprehensive reports are developed to ensure that observed issues are identified in the after action report.
	(l)(2)(v) Licensees shall enter all findings, deficiencies, and failures identified by each performance evaluation into the corrective action program to ensure that timely corrections are made to the onsite physical protection program and necessary changes are made to the approved security plans, licensee protective strategy, and implementing procedures.	This requirement would be added to ensure that corrective action plans are developed and tracked to provide resolution.
	(l)(2)(vi) Licensees shall protect all findings, deficiencies, and failures relative to the effectiveness of the onsite physical protection program in accordance with the requirements of § 73.21.	This requirement would be added to provide for the appropriate level of protection for the type of information being developed. Information involving findings, deficiencies and failures is considered sensitive and must be protected accordingly.
	(l)(3) For the purpose of drills and exercises, licensees shall:	This new header would be added for formatting purposes.

	(l)(3)(i) Use no more than the number of armed personnel specified in the approved security plans to demonstrate effectiveness.	This requirement would be added to ensure that realistic tests are conducted against those forces available onsite on a routine basis. Conducting drills under other than with actual or non typical staffing levels would not provide for accurate system effectiveness determinations.
	(l)(3)(ii) Minimize the number and effects of artificialities associated with drills and exercises.	This requirement would be added to ensure that exercises are conducted as realistically as possible. Artificialities if not minimized would result in inaccurate system effectiveness determinations.
	(l)(3)(iii) Implement the use of systems or methodologies that simulate the realities of armed engagement through visual and audible means, and reflects the capabilities of armed personnel to neutralize a target though the use of firearms during drills and exercises.	This requirement would be added to provide for the utilization of technological advancements for simulating live fire combat situations in a controlled environment. These may include but are not limited to the use of laser engagement systems or dye marking cartridges.
	(l)(3)(iv) Ensure that each scenario used is capable of challenging the ability of armed personnel to perform assigned duties and implement required elements of the protective strategy.	This requirement would be added to ensure that scenarios are developed to stress the protective strategy in manner that deficiencies or weaknesses can be identified.
	(l)(4) The Performance Evaluation Program must be designed to ensure that:	This requirement would be added to improve the usefulness and applicability of the safeguards contingency plan.

	(l)(4)(i) Each member of each shift who is assigned duties and responsibilities required to implement the approved safeguards contingency plan and licensee protective strategy participates in at least one (1) drill on a quarterly basis and one (1) force on force exercise on an annual basis.	This requirement would be added to ensure that individual members of the security force participate in drills at a frequency that provides them with knowledge and performance based experience applying the protective strategy.
	(l)(4)(ii) The mock adversary force replicates, as closely as possible, adversary characteristics and capabilities in the design basis threat described in § 73.1(a)(1), and is capable of exploiting and challenging the licensee protective strategy, personnel, command and control, and implementing procedures.	This requirement would be added to ensure that the mock adversary force is capable of portraying the design basis threat in terms of size, activity, movement, tactics, equipment and weaponry.
	(l)(4)(iii) Protective strategies are evaluated and challenged through tabletop demonstrations.	This requirement would be added to provide an opportunity to evaluate protective strategies focusing on incident command in an open discussion format.
	(l)(4)(iv) Drill and exercise controllers are trained and qualified to ensure each controller has the requisite knowledge and experience to control and evaluate exercises.	This requirement would be added to ensure the use of qualified controllers who are knowledgeable of safety, environmental conditions, hazards, tactics, weapons equipment, and physical security systems.
	(l)(4)(v) Drills and exercises are conducted safely in accordance with site safety plans.	This requirement would be added to ensure licensee safety plans are considered in the conduct of drills and exercises.

	(l)(5) 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.	This requirement would be added to ensure that the mock adversary force is not influenced by security management or personnel responsible for security. This mitigates the potential for the scenario to be compromised or not carried out to the desired expectation. This proposed requirement is based on the EPAct 2005 section 651.
	(l)(6) Scenarios.	
	(l)(6)(i) Licensees shall develop and document multiple scenarios for use in conducting quarterly drills and annual force-on-force exercises.	This requirement would be added to ensure that varying scenarios with differing adversary configurations are used against all target sets for increased readiness. This permits a better determination of overall system effectiveness.
	(l)(6)(ii) Licensee scenarios must be designed to test and challenge any component or combination of components, of the onsite physical protection program and protective strategy.	This requirement would be added to ensure that scenarios are developed in a manner that each aspect of the security system and strategy will be analyzed to determine effectiveness.

	(l)(6)(iii) 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.	This requirement would be added to ensure that scenarios are developed in a manner that each aspect of the security system and strategy will be analyzed to determine overall system effectiveness.
	(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 years (3) for exercises.	This requirement would be added to ensure the development of scenarios with differing adversary configurations against varying target sets. This promotes increased readiness and permits a better determination of overall system effectiveness.
Audit and Review.	(m) Records, audits, and reviews.	This header would be retained and revised to add records retention requirements.

App. C 5.(1) For nuclear power reactor licensees subject to the requirements of § 73.55, the licensee shall provide for a review of the safeguards contingency plan either: App. C 5.(1)(i) At intervals not to exceed 12 months, or... App. C 5.(1)(ii) As necessary, based on an assessment by the licensee against performance indicators, and as soon as reasonably practicable after a change occurs in personnel, procedures, equipment, or facilities that potentially could adversely affect security, but no longer than 12 months after the change. App. C 5.(1)(ii) ...In any case, each element of the safeguards contingency plan must be reviewed at least every 24 months. App. C 5.(2) A licensee subject to the requirements of either § 73.46 or § 73.55, shall ensure that the review of the safeguards contingency plan is by individuals independent of both security	(m)(1) Licensees shall review and audit the Commission-approved safeguards contingency plan in accordance with the requirements § 73.55(n) of this part.	This requirement would be revised to ensure that the protective strategy is revised as a result of any significant changes that would effect the ability to respond in accordance with the existing contingency plan.

program management and personnel who have direct responsibility for implementation of the security program. Appendix C Paragraph 5(3). The licensee shall document the results and the recommendations of the safeguards contingency plan review, management findings on whether the safeguards contingency plan is currently effective, and any actions taken as a result of recommendations from prior reviews in a report to the licensee's plant manager and to corporate management at least one level higher than that having responsibility for the day-to-day plant operation.		
Appendix C Paragraph 5.(2) The review must include an audit of safeguards contingency procedures and practices, and an audit of commitments established for response by local law enforcement authorities.	(m)(2) The licensee shall make necessary adjustments to the Commission-approved safeguards contingency plan to ensure successful implementation of Commission regulations and the site protective strategy.	This requirement would be revised to ensure that the protective strategy is revised as a result of any significant changes that would affect the ability to respond in accordance with the existing contingency plan.
Appendix C Paragraph 5.(2) The review must include an audit of safeguards contingency procedures and practices, and an audit of commitments established for response by local law enforcement authorities.	(m)(3) The safeguards contingency plan review must include an audit of implementing procedures and practices, the site protective strategy, and response agreements made by local, state, and Federal law enforcement authorities.	This requirement would be revised to ensure that an audit of the safeguards contingency plan is conducted to validate essential aspects of the plan.

Appendix C Paragraph 5.(3) The report must be maintained in an auditable form, available for inspection for a period of 3 years.	(m)(4) Licensees shall retain all reports, records, or other documentation required by this appendix in accordance with the requirements of § 73.55(r).	This requirement would be added to improve the usefulness and applicability of the safeguards contingency plan.
Appendix C Paragraph 5. Procedures	(n) Implementing procedures.	This requirement would be retained with editorial changes. The word “Implementing” has been added to further define the requirement.
In order to aid execution of the detailed plan as developed in the Responsibility Matrix, this category of information shall detail the actions to be taken and decisions to be made by each member or unit of the organization as planned in the Responsibility Matrix. Contents of the Plan: Although the implementing procedures (the fifth category of Plan information) are the culmination of the planning process, and therefore are an integral and important part of the safeguards contingency plan, they entail operating details subject to frequent changes.	(n)(1) 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 Commission-approved security plans and the site protective strategy.	This requirement would be revised to ensure that plans are developed to cover security force routine, emergency, administrative, and other operational duties.
Contents of the Plan: The licensee is responsible for ensuring that the implementing procedures reflect the information in the Responsibility Matrix, appropriately summarized and suitably presented for effective use by the responding entities.	(n)(2) Licensees shall ensure that implementing procedures accurately reflect the information contained in the Responsibility Matrix required by this appendix, the Commission-approved security plans, the Integrated Response Plan, and other site plans.	This requirement would be revised to ensure that plans are developed to cover security force routine, emergency, administrative, and other operational duties. The phrase "appropriately summarized and suitably presented for effective use by the responding entities" would be deleted because this concept would be covered under demonstration.

Contents of the Plan: They need not be submitted to the Commission for approval, but will be inspected by NRC staff on a periodic basis.	(n)(3) Implementing procedures need not be submitted to the Commission for approval but are subject to inspection.	This requirement would be retained with editorial changes.

Table 8 - Part 73 Appendix G
Reportable safeguards events.

CURRENT LANGUAGE	PROPOSED LANGUAGE	CONSIDERATIONS
[Introductory text to App. G] Pursuant to the provisions of 10 CFR 73.71 (b) and (c), licensees subject to the provisions of 10 CFR 73.20, 73.37, 73.50, 73.55, 73.60, and 73.67 shall report or record, as appropriate, the following safeguards events.	[Introductory text to App. G] Under the provisions of § 73.71(a), (d), and (f) of this part, licensees subject to the provisions of §73.55 of this part shall report or record, as appropriate, the following safeguards events under paragraphs I, II, III, and IV of this appendix. Under the provisions of § 73.71(b), (c), and (f) of this part, licensees subject to the provisions of §§ 73.20, 73.37, 73.50, 73.60, and 73.67 of this part shall report or record, as appropriate, the following safeguards events under paragraphs II and IV of this appendix. Licensees shall make such reports to the Commission under the provisions of § 73.71 of this part.	This appendix would be revised by adding new requirements for nuclear power reactor licensees. Power reactor licensees subject to the provisions of § 73.55 would be required to notify the Commission (1) within 15 minutes after discovery of an imminent or actual threat against the facility and (2) within four hours of discovery of suspicious events. The proposed 15-minute requirement would more accurately reflect the current threat environment. Because an actual or potential threat could quickly result in an event, a shorter reporting time would be required. However, the requirement for Commission notification within 15 minutes would be applied only to nuclear power reactor licensees, at this time. The Commission may consider the applicability of this requirement to other licensees in future rulemaking. The new 4-hour notification would be intended to aid the Commission, law enforcement, and the intelligence community is assessing suspicious activity that may indicative of pre-operational surveillance, reconnaissance, or intelligence gathering efforts.

		Events reported under paragraphs I or II would require a followup written report. Events reported under paragraph III would not require a followup written report.
	I. Events to be reported as soon as possible, but no later than 15 minutes after discovery, followed by a written report within sixty (60) days. (a) The initiation of a security response consistent with a licensee's physical security plan, safeguards contingency plan, or defensive strategy based on actual or imminent threat against a nuclear power plant.	Paragraph I would be added to establish the types events to be reported within 15 minutes. Because the identification of information relating to an actual or imminent threat could quickly result in an event, which may necessitate expedited Commission action (e.g., notification of other licensees or Federal authorities), a shortened reporting time would be required. This proposed requirement would also ensure that threat-related information would be made available to the Commission's threat assessment process in a timely manner. Initiation of response consistent with plans and the defensive strategy that are not related to an imminent or actual threat against the facility would not need to be reported (e.g false, or nuisance responses). Additional information regarding identification of events to be reported would be provided in guidance.
	I.(b) The licensee is not required to report security responses initiated as a result of information communicated to the licensee by the Commission, such as the threat warning system addressed in appendix C to this part.	This provision would be added to reduce unnecessary regulatory burden on the licensees to notify the Commission of security responses initiated in response to communications from the Commission (e.g., changes to the threat level).

I. Events to be reported within one hour of discovery, followed by a written report within 60 days.	II. Events to be reported within one (1) hour of discovery, followed by a written report within sixty (60) days.	This requirement would be retained and renumbered.
(a) Any event in which there is reason to believe that a person has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause:	II.(a) Any event in which there is reason to believe that a person has committed or caused, or attempted to commit or cause, or has made a threat to commit or cause:	This requirement would be retained with minor revision and renumbered. The term credible would be removed. The Commission's view is that a determination of the "credibility" of a threat is not a licensee responsibility, but rests with the Commission and the intelligence community.
(1) A theft or unlawful diversion of special nuclear material; or	II.(a)(1) A theft or unlawful diversion of special nuclear material; or	This requirement would be retained and renumbered.
(2) Significant physical damage to a power reactor or any facility possessing SSNM or its equipment or carrier equipment transporting nuclear fuel or spent nuclear fuel, or to the nuclear fuel or spent nuclear fuel a facility or carrier possesses; or	II.(a)(2) Significant physical damage to any NRC-regulated power reactor or facility possessing strategic special nuclear material or to carrier equipment transporting nuclear fuel or spent nuclear fuel, or to the nuclear fuel or spent nuclear fuel facility which is possessed by a carrier; or	This requirement would be retained with minor editorial changes to improve clarity and readability and renumbered. The phrase "NRC-regulated" would be added to specify that all Commission licensed facilities and transport would be covered by this requirement. This change would simplify the language in this section while retaining the basic requirement.

(3) Interruption of normal operation of a licensed nuclear power reactor through the unauthorized use of or tampering with its machinery, components, or controls including the security system.	II.(a)(3) Interruption of normal operation of any NRC-licensed nuclear power reactor through the unauthorized use of or tampering with its components, or controls including the security system.	This requirement would be retained with minor revision and renumbered. The word “machinery” would be deleted since “components” includes machinery and other physical structures at a licensed facility. This proposed requirement would continued to be applied only to nuclear power reactors licensed by the Commission, at this time. The Commission may consider the applicability of this requirement to other classes of licensees in future rulemaking.
(b) An actual entry of an unauthorized person into a protected area, material access area, controlled access area, vital area, or transport.	II.(b) An actual or attempted entry of an unauthorized person into any area or transport for which the licensee is required by Commission regulations to control access.	This requirement would be renumbered and revised to delete the previously specifically mentioned areas (“protected area, material access area, controlled access area, vital area”) requiring access controls and change the language to include the actual or attempted entry of an unauthorized individual into any area required to be controlled by Commission regulations. This change would more accurately reflect the current threat environment.

		The revision also reflects Commission experience with implementation of the 2003 security order's requirements and review of revised license security plans. Licensee's defensive strategies and revised Safeguards Contingency Plans have introduced additional significant locations (e.g. target sets) that may not be limited to the previously specified areas. Additional information regarding identification of events to be reported will be provided in guidance.
(c) Any failure, degradation, or the discovered vulnerability in a safeguard system that could allow unauthorized or undetected access to a protected area, material access area, controlled access area, vital area, or transport for which compensatory measures have not been employed.	II.(c) Any failure, degradation, or the discovered vulnerability in a safeguard system that could allow unauthorized or undetected access to any area or transport for which the licensee is required by Commission regulations to control access and for which compensatory measures have not been employed.	This requirement would be renumbered and revised to delete the previously specifically mentioned areas ("protected area, material access area, controlled access area, vital area") requiring access controls and to broaden the language to include any area required to be controlled by the Commission regulations (see considerations for paragraph II.(b) above). Additional information regarding identification of events to be reported will be provided in guidance.

(d) The actual or attempted introduction of contraband into a protected area, material access area, vital area, or transport.	II.(d) The actual or attempted introduction of contraband into any area or transport for which the licensee is required by Commission regulations to control access.	This requirement would be renumbered and revised to delete the previously specifically mentioned areas requiring access controls and change the language to include the actual or attempted entry of an unauthorized individual into any area or transport required to be controlled by Commission regulations (see considerations for paragraph II.(b) above). Additional information regarding identification of events to be reported will be provided in guidance.
NRC Information Assessment Team (IAT) Advisories dated October 16, and November 15, 2001; May 20, 2003; March1, 2004; and October 5, 2005. FBI's "Terrorist Threats to the U.S. Homeland: Reporting Guide for Critical and Key Resource Owners and Operators" dated January 24, 2005, (Official Use Only).	III. Events to be reported within four (4) hours of discovery. No written followup report is required. (a) Any other information received by the licensee of suspicious surveillance activities or attempts at access, including: (1) Any security-related incident involving suspicious activity that may be indicative of potential pre-operational surveillance, reconnaissance, or intelligence-gathering activities directed against the facility. Such activity may include, but is not limited to,	This paragraph would add a requirement for power reactor licensees to report suspicious activities, attempts at access, etc., that may indicate pre-operational surveillance, reconnaissance, or intelligence gathering targeted against the facility. This change would more accurately reflect the current threat environment; would assist the Commission in evaluating threats to multiple licensees; and would assist the intelligence and homeland security communities in evaluating threats

	attempted surveillance or reconnaissance activity, elicitation of information from security or other site personnel relating to the security or safe operation of the plant, or challenges to security systems (e.g., failure to stop for security checkpoints, possible tests of security response and security screening equipment, or suspicious entry of watercraft into posted off-limits areas). (2) Any security-related incident involving suspicious aircraft overflight activity. Commercial or military aircraft activity considered routine by the licensee is not required to be reported.	across critical infrastructure sectors. The reporting process intended in this proposed rule would be similar reporting process that the licensees currently use under guidance issued by the Commission subsequent to September 11, 2001, and would formalize Commission expectations; however, the reporting interval would be lengthened from 1 hour to 4 hours. The Commission views this length of time as reasonable to accomplish these broader objectives. This reporting requirement does not include a followup written report. The Commission believes that a written report from the licensees would be of minimal value and would be an unnecessary regulatory burden, because the types of incidents to be reported are transitory in nature and time-sensitive. The proposed text would be neither a request for intelligence collection activities nor authority for the conduct of law enforcement or intelligence activities. This paragraph would simply require the reporting of observed activities.

		Paragraphs III(a)(1) and (2) provide broad examples of events that should be reported, or need not be reported. Additional information regarding identification of events to be reported will be provided in guidance. The Commission may consider the applicability of this requirement to other licensees in future rulemaking.
	III.(a)(3) Incidents resulting in the notification of local, state or national law enforcement, or law enforcement response to the site not included in paragraphs I or II of this appendix;	This paragraph would be added to establish a performance standard for additional types of incidents or activities involving law enforcement authorities not otherwise specified in paragraphs I and II of this appendix. Additional information regarding identification of events to be reported will be provided in guidance.
	III.(b) The unauthorized use of or tampering with the components or controls, including the security system, of nuclear power reactors.	This paragraph would be added to address “tampering” events that do not rise to the significance of affecting plant operations as specified in paragraph II.(a)(3) and would use similar language to the proposed paragraph II.(a)(3).

	III.(c) Follow-up communications regarding these incidents will be completed through the NRC threat assessment process via the NRC Operations Center.[1] Footnote: 1. Commercial (secure and non-secure) telephone numbers of the NRC Operations Center are specified in appendix A of this part.	This requirement would be added to establish a performance standard for any follow-up communication between licensees and the Commission regarding the initial report of "suspicious" activity. This process has been set forth in guidance documents and the Commission intends that licensees would continue to implement the existing process with little change.
II. Events to be recorded within 24 hours of discovery in the safeguards event log.	IV. Events to be recorded within 24 hours of discovery in the safeguards event log.	This requirement would be retained and renumbered.
(a) Any failure, degradation, or discovered vulnerability in a safeguards system that could have allowed unauthorized or undetected access to a protected area, material access area, controlled access area, vital area, or transport had compensatory measures not been established.	IV.(a) Any failure, degradation, or discovered vulnerability in a safeguards system that could have allowed unauthorized or undetected access to any area or transport in which the licensee is required by Commission regulations to control access had compensatory measures not been established.	The current requirement would be renumbered and revised to revised to delete the previously specifically mentioned areas ("protected area, material access area, controlled access area, vital area") requiring access controls and change the language to include the actual or attempted entry of an unauthorized individual into any area required to be controlled by Commission regulations (see considerations for paragraph II.(b) above). Additional information regarding identification of events to be recorded will be provided in guidance.

(b) Any other threatened, attempted, or committed act not previously defined in appendix G with the potential for reducing the effectiveness of the safeguards system below that committed to in a licensed physical security or contingency plan or the actual condition of such reduction in effectiveness.	IV.(b) Any other threatened, attempted, or committed act not previously defined in this appendix with the potential for reducing the effectiveness of the physical protection program below that described in a licensee physical security or safeguards contingency plan, or the actual condition of such a reduction in effectiveness.	This requirement would be renumbered and retained with minor revisions. This paragraph would be changed to replace “the physical protection system” with “the safeguards system” and “described” for “committed.” These changes would reflect Commission experience with implementation of security order requirements and reviews of revisions to licensee security plans.

V. Guidance

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

VI. Criminal Penalties

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

VII. Compatibility of Agreement State Regulations

Under the "Policy Statement on Adequacy and Compatibility of Agreement States Programs," approved by the Commission on June 20, 1997, and published in the Federal Register (62 FR 46517; September 3, 1997), this rule is classified as compatibility "NRC." Compatibility is not required for Category "NRC" regulations. The NRC program elements in this

category are those that relate directly to areas of regulation reserved to the NRC by the AEA or the provisions of Title 10 of the Code of *Federal Regulations* (10 CFR), and although an Agreement State may not adopt program elements reserved to NRC, it may wish to inform its licensees of certain requirements via a mechanism that is consistent with the particular State's administrative procedure laws, but does not confer regulatory authority on the State.

VIII. Availability of Documents.

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

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

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

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

Document	**PDR**	**Web**	**ERR** (ADAMS)
Environmental Assessment	x	x	ML061920093
Regulatory Analysis Regulatory Analysis -appendices	x	x	ML061920012 ML061380796 ML061440013
Information Collection Analysis	x	x	ML062340362 ML062830016
NRC Form 754	x	x	ML060930319
Memorandum: Status of Security-Related Rulemaking (July 19, 2004)	x	x	ML041180532
Commission SRM (August 23, 2004)	x	x	ML042360548

Document	PDR	Web	ERR (ADAMS)
Memorandum: Schedule for Part 73 Rulemakings (November 16, 2004)	x	x	ML043060572
Revised Schedule for Completing Part 73 rulemaking (July 29, 2005)	x	x	ML051800350
COMSECY-05-0046 (September 29, 2005)	x	x	ML052710167
SRM on COMSECY-05-0046 (November 1, 2005)	x	x	ML053050439
EA-02-026, “Interim Compensatory Measures (ICM) Order”(67 FR 9792)	x	x	ML020520754
EA-02-261, “Issuance of Order for Compensatory Measures Related to Access Authorization” (68 FR 1643)	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” (68 FR 24514)	x	x	ML030980015
NRC Bulletin 2005-02, “Emergency Preparedness and Response Actions for Security-based Events”	x	x	ML051740058
Petition for Rulemaking (PRM-50-80)	x	x	ML031681105
SECY-05-0048, Petition for Rulemaking on Protection of U.S. Nuclear Power Plants Against Radiological Sabotage (PRM-50-80)	x	x	ML051790404
SRM-SECY-05-0048, Staff Requirements on SECY-05-0048	x	x	ML053000500
Table 9 Cross-walk table for proposed § 73.55.	x	x	ML060910004

Document	PDR	Web	ERR (ADAMS)
Table 10 Cross-walk table for proposed 10 CFR part 73 appendix B.	x	x	ML060910006
Table 11 Cross-walk table for proposed 10 CFR part 73 appendix C.	x	x	ML060910007

IX. Plain Language.

The Presidential memorandum dated June 1, 1998, entitled "Plain Language in Government Writing" directed that the Government's writing be in plain language. This memorandum was published on June 10, 1998 (63 FR 31883). In complying with this directive, the NRC made editorial changes to improve the organization and readability of the existing language of the paragraphs being revised. These types of changes are not discussed further in this document. The NRC has used the phrase "may not" throughout this proposed rule to indicate that a person or entity is prohibited from taking a specific action. The NRC requests comments on the proposed rule specifically with respect to the clarity and reflectiveness of the language used. Comments should be sent to the address listed under the ADDRESSES caption of the preamble.

X. Voluntary Consensus Standards.

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

XI. 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, if adopted, would not be a major Federal action significantly affecting the quality of the human environment and, therefore, an environmental impact statement is not required.

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

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

XII. Paperwork Reduction Act Statement.

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

Type of submission, new or revision: Revision and new.

The title of the information collection: 10 CFR part 73, “Power Reactor Security Requirements” proposed rule, and NRC Form 754, “Armed Security Personnel Background Check.”

The form number if applicable: NRC Form 754.

How often the collection is required: Collections will be initially required due to the need for power reactor licensees to revise security plans and submit the plans for staff review and approval. New records requirements are imposed to: document target sets in

procedures, maintain records of storage locations for unirradiated MOX fuel, document the onsite physical protection system review, document problems and deficiencies, implement a cyber security program including the requirement to develop associated implementing procedures, implement a cyber incident response and recovery plan, implement a cyber security awareness and training plan, and implement the access authorization program. New annual collection requirements will be imposed including requirements to maintain a record of all individuals to whom access control devices were issued. Collections will also be required on a continuing basis due to new proposed reporting requirements which include: to notify the NRC within 72 hours of taking action to remove security personnel per proposed § 73.18, to notify the NRC within 15 minutes after discovery of an imminent threat or actual safeguards threat against the facility including a requirement to follow this report with a written report within 60 days, and a requirement to report to NRC within 4 hours of incidents of suspicious activity or tampering. A new NRC form 754 background check would be required to be completed by all security personnel to be assigned armed duties.

Who will be required or asked to report: Power reactor licensees will be subject to all the proposed requirements in this rulemaking. Category I special nuclear material facilities will be required to report for only the collections in proposed § 73.18 and § 73.19.

An estimate of the number of annual responses: 10 CFR Part 73 - 15,156 (8,523 annualized one-time plus 6, 644 annual responses).

The estimated number of annual respondents: 65 to 68 and, additionally, decommissioning sites for §73.55(a)(1).

An estimate of the total number of hours needed annually to complete the requirement or request: 10 CFR 73 - 145,613 hours (84,190 hours annualized one-time and 49,013 hours annual recordkeeping [732 hours per recordkeeper] plus 821 hours annualized

one-time and 11,590 hours annual reporting [173 hours per licensee]; NRC form 754 - 1,250 hours (or an average of 18.7 hours per site) for one-time collections and 261 hours (or an average of 3.9 hours per site) annually.

Abstract: The Nuclear Regulatory Commission (NRC) is proposing to amend the current security regulations and add new security requirements pertaining to nuclear power reactors. Additionally, this rulemaking includes new security requirements for Category I strategic special nuclear material (SSNM) facilities for access to enhanced weapons and firearms background checks. The proposed rulemaking would: (1) 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, (2) fulfill certain provisions of the Energy Policy Act of 2005, (3) add several new requirements that resulted from insights from implementation of the security orders, review of site security plans, and implementation of the enhanced baseline inspection program and force-on-force exercises, (4) update the regulatory framework in preparation for receiving license applications for new reactors, and (5) impose requirements to assess and manage site activities that can adversely affect safety and security.

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

1. Is the proposed information collection necessary for the proper performance of the functions of the NRC, including whether the information will have practical utility?
2. Estimate of burden?
3. Is there a way to enhance the quality, utility, and clarity of the information to be collected?

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

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

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

XIII. Public Protection Notification

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

XIV. Regulatory Analysis.

The Commission has prepared a draft regulatory analysis on this proposed regulation. The analysis examines the costs and benefits of the alternatives considered by the Commission.

The Commission requests public comments on the draft regulatory analysis. Availability of the regulatory analysis is provided in Section VIII. Comments on the draft analysis may be submitted to the NRC as indicated under the ADDRESSES heading.

XV. Regulatory Flexibility Certification.

In accordance with the Regulatory Flexibility Act (5 U.S.C. 605(b)), the Commission certifies that this rule would not, if promulgated, have a significant economic impact on a substantial number of small entities. This proposed rule affects only the licensing and operation of nuclear power plants, production facilities, spent fuel reprocessing or recycling facilities, fuel fabrication facilities, and uranium enrichment facilities. 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).

XVI. Backfit Analysis.

The NRC evaluated the aggregated set of requirements in this proposed rulemaking that constitute backfits in accordance with 10 CFR 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 proposed part 73 rule provisions that qualify as backfits in this proposed 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 VIII.

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 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; and 5 U.S.C. 553; the NRC is proposing to adopt the following amendments to 10 CFR Parts 50, 72, and 73.

PART 50--DOMESTIC LICENSING OF PRODUCTION AND UTILIZATION FACILITIES

1. The authority citation for part 50 is revised 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); Energy Policy Act of 2005, Pub. L. No. 109-58, 119 Stat. 594 (2005). Section 50.7 also issued under Pub. L. 95-601, sec. 10, 92 Stat. 2951 (42 U.S.C. 5841). Section 50.10 also issued under secs. 101, 185, 68 Stat. 955, as amended (42 U.S.C. 2131, 2235); sec.

102, Pub. L. 91-190, 83 Stat. 853 (42 U.S.C. 4332). Sections 50.13, 50.54(dd), and 50.103 also issued under sec. 108, 68 Stat. 939, as amended (42 U.S.C. 2138).

Sections 50.23, 50.35, 50.55, and 50.56 also issued under sec. 185, 68 Stat. 955 (42 U.S.C. 2235). Sections 50.33a, 50.55a and appendix Q also issued under sec. 102, Pub. L. 91-190, 83 Stat. 853 (42 U.S.C. 4332). Sections 50.34 and 50.54 also issued under sec. 204, 88 Stat. 1245 (42 U.S.C. 5844). Sections 50.58, 50.91, and 50.92 also issued under Pub. L. 97-415, 96 Stat. 2073 (42 U.S.C. 2239). Section 50.78 also issued under sec. 122, 68 Stat. 939 (42 U.S.C. 2152). Sections 50.80 - 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, and paragraph (d) is revised to read as follows:

§ 50.34 Contents of applications; technical information.

* * * * *

(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 “Implementation Procedures” required in section II(g)(12) of appendix C to part 73 of this chapter do not have to be submitted to the Commission for approval.

* * * * *

3. In § 50.54, paragraph (p)(1) is revised 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 make no change which would decrease the effectiveness of a physical security plan, or guard training and qualification plan, prepared under § 50.34(c) or part 73 of this chapter, or of any category of information with the exception of the "Implementation Procedures" category contained in a licensee safeguards contingency plan prepared under § 50.34(d) 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 an amendment to the licensee's license under § 50.90. * * * * *

4. In § 50.72, paragraph (a), footnote 1 is revised and the heading of paragraph (a) is republished for the convenience of the user to read as follows:

§ 50.72 Immediate notification requirements for operating nuclear power reactors.

(a) General Requirements.[1] * * *

* * * * *

---

[1] Other requirements for immediate notification of the NRC by licensed operating nuclear power reactors are contained elsewhere in this chapter, in particular §§ 20.1906, 20.2202, 50.36, 72.216, and 73.71, and may require NRC notification before that required under § 50.72.

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

5. The authority citation for part 72 is revised 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); Energy Policy Act of 2005, Pub. L. No. 109-58, 119 Stat. 549 (2005).

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).

6. 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)(7) of this chapter as applied to a new protected area may be provided by a guard or watchman on patrol in lieu of closed circuit television.

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

* * * * *

PART 73 - PHYSICAL PROTECTION OF PLANTS AND MATERIALS

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

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.S.C. 5841, 5844, 2297f); sec. 1704, 112

Stat. 2750 (44 U.S.C. 3504 note); Energy Policy Act of 2005, Pub. L. No. 109-58, 119 Stat. 594 (2005).

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

8. In § 73.2, definitions for *covered weapon*, *enhanced weapon*, *safety/security interface*, *security officer*, *standard weapon*, and *target set* are added in alphabetical order to read as follows:

§ 73.2 Definitions.

* * * * *

Covered weapon means any handgun, rifle, shotgun, short-barreled shotgun, short-barreled rifle, semi-automatic assault weapon, machinegun, ammunition for any such gun or weapon, or a large capacity ammunition feeding device as specified under section 161A of the Atomic Energy Act of 1954, as amended. As used here, the terms "handgun, rifle, shotgun, short-barreled shotgun, short-barreled rifle, semi-automatic assault weapon, machinegun, ammunition, or large capacity ammunition feeding device" have the same meaning as set forth for these terms under 18 U.S.C. 921(a). Covered weapons include both enhanced weapons and standard weapons. However, enhanced weapons do not include standard weapons.

* * * * *

Enhanced weapon means any short-barreled shotgun, short-barreled rifle, or machinegun. Enhanced weapons do not include destructive devices, including explosives or weapons greater than 50 caliber (i.e., weapons with a bore greater than 1.27 cm [0.5 in] diameter).

* * * * *

Safety/Security interface (SSI) means the actual or potential interactions that may adversely affect security activities due to any operational activities, or vice versa.

* * * * *

Security officer means a uniformed individual, either armed with a covered weapon or unarmed, whose primary duty is the protection of a facility, of radioactive material, or of other property against theft or diversion or against radiological sabotage.

* * * * *

Standard weapon means any handgun, rifle, shotgun, semi-automatic assault weapon, or a large capacity ammunition feeding device.

* * * * *

Target set means 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 (e.g., non-incipient, non-localized fuel melting, and/or core disruption) barring extraordinary action by plant operators. A target set with respect to spent fuel sabotage is draining the spent fuel pool leaving the spent fuel uncovered for a period of time, allowing spent fuel heat up and the associated potential for release of fission products.

* * * * *

9. 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, 73.18, 73.19, 73.20, 73.21, 73.24, 73.25, 73.26, 73.27, 73.37, 73.40, 73.45, 73.46, 73.50, 73.55, 73.56, 73.57, 73.58, 73.60, 73.67, 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. These information collection requirements and control numbers under which they are approved are as follows:

(1) In § 73.18, NRC Form 754 is approved under control number 3150-xxxx;

(2) In § 73.71, NRC Form 366 is approved under control number 3150-0104; and

(3) In §§ 73.18 and 73.57, Form FD-258 is approved under control number 1110-yyyy.

10. Section 73.18 is added to read as follows:

§ 73.18 Firearms background check for armed security personnel.

(a) *Purpose*. This section sets forth the requirements for completion of firearms background checks on armed security personnel at selected NRC-regulated facilities. Firearms background checks are intended to verify that armed security personnel whose duties require access to covered weapons are not prohibited from receiving, possessing, transporting, importing, or using such weapons under applicable Federal or State law. Licensees and certificate holders listed under paragraph (c) of this section who have applied for preemption authority under § 73.19 (i.e., § 73.19 authority), or who have been granted preemption authority by Commission order, are subject to the requirements of this section.

(b) *General Requirements*. (1) Licensees and certificate holders listed in paragraph (c) of this section who have received NRC approval of their application for preemption authority shall ensure that a firearms background check has been satisfactorily completed for all security personnel requiring access to covered weapons as part of their official security duties prior to granting access to any covered weapons to those personnel. Security personnel who have

satisfactorily completed a firearms background check, but who have had a break in employment with the licensee, certificate holder, or their security contractor of greater than one (1) week subsequent to their most recent firearms background check, or who have transferred from a different licensee or certificate holder (even though the other licensee or certificate holder satisfactorily completed a firearms background check on such individuals), are not excepted from the requirements of this section.

(2) Security personnel who have satisfactorily completed a firearms background check pursuant to Commission orders are not subject to a further firearms background check under this section, unless these personnel have a break in service or transfer as set forth in paragraph (b)(1) of this section.

(3) A change in the licensee, certificate holder, or ownership of a facility, radioactive material, or other property designated under § 73.19, or a change in the security contractor that provides security personnel responsible for protecting such facilities, radioactive material, or other property, shall not constitute 'a break in service' or 'transfer,' as those terms are used in paragraph (b)(2) of this section.

(4) Licensees and certificate holders listed in paragraph (c) of this section may begin the application process for firearms background checks under this section for security personnel whose duties require access to covered weapons immediately on application to the NRC for preemption authority.

(5) Firearms background checks do not replace any other background checks or criminal history checks required for the licensee's or certificate holder's security personnel under this chapter.

(c) *Applicability*. This section applies to licensees or certificate holders who have applied for or received NRC approval of their application for § 73.19 authority or were issued Commission orders requiring firearms background checks.

(d) *Firearms background check requirements*. A firearms background check for security personnel must include –

(1) A check of the individual's fingerprints against the Federal Bureau of Investigation's (FBI's) fingerprint system; and

(2) A check of the individual's identifying information against the FBI's National Instant Criminal Background Check System (NICS).

(e) *Firearms background check submittals*. (1) Licensees and certificate holders shall submit to the NRC, in accordance with § 73.4, for all security personnel requiring a firearms background check under this section -

(i) A set of fingerprints, in accordance with paragraph (o) of this section, and

(ii) A completed NRC Form 754.

(2) Licensees and certificate holders shall retain a copy of all NRC Forms 754 submitted to the NRC for a period of one (1) year subsequent to the termination of an individual's access to covered weapons or to the denial of an individual's access to covered weapons.

(f) *NICS portion of a firearms background check*. The NRC will forward the information contained in the submitted NRC Forms 754 to the FBI for evaluation against the NICS. Upon completion of the NICS portion of the firearms background check, the FBI will inform the NRC of the results with one of three responses under 28 CFR part 25; "proceed," "denied," or "delayed," and the associated NICS transaction number. The NRC will forward these results and the associated NICS transaction number to the submitting licensee or certificate holder. The submitting licensee or certificate holder shall provide these results to the individual who completed the NRC Form 754.

(g) *Satisfactory and adverse firearms background checks*. (1) A satisfactorily completed firearms background check means a "proceed" response for the individual from the FBI's NICS.

(2) An adversely completed firearms background check means a “denied” or “delayed” response from the FBI's NICS.

(h) *Removal from access to covered weapons*. Licensees or certificate holders who have received NRC approval of their application for § 73.19 authority shall ensure security personnel are removed from duties requiring access to covered weapons upon the licensee's or certificate holder's knowledge of any disqualifying status or the occurrence of any disqualifying events under 18 U.S.C. 922(g) or (n), and the ATF’s implementing regulations in 27 CFR part 478.

(i) [Reserved].

(j) *Security personnel responsibilities*. Security personnel assigned duties requiring access to covered weapons shall promptly [within three (3) working days] notify their employing licensee’s or certificate holder’s security management (whether directly employed by the licensee or certificate holder or employed by a security contractor to the licensee or certificate holder) of the existence of any disqualifying status or upon the occurrence of any disqualifying events listed under 18 U.S.C. 922(g) or (n), and the ATF’s implementing regulations in 27 CFR part 478 that would prohibit them from possessing or receiving a covered weapon.

(k) *Awareness of disqualifying events*. Licensees and certificate holders who have received NRC approval of § 73.19 authority shall include within their NRC-approved security training and qualification plans instruction on –

(1) Disqualifying status or events specified in 18 U.S.C. 922(g) and (n), and ATF’s implementing regulations in 27 CFR part 478 (including any applicable definitions) identifying categories of persons who are prohibited from possessing or receiving any covered weapons; and

(2) The continuing responsibility of security personnel assigned duties requiring access to covered weapons to promptly notify their employing licensee or certificate holder of the occurrence of any disqualifying events.

(l) [Reserved].

(m) *Notification of removal*. Within 72 hours after taking action to remove security personnel from duties requiring access to covered weapons, because of the existence of any disqualifying status or the occurrence of any disqualifying event – other than due to the prompt notification by the security officer under paragraph (j) of this section – licensees and certificate holders who have received NRC approval of § 73.19 authority shall notify the NRC Operations Center of such removal actions, in accordance with appendix A of this part.

(n) *Reporting violations of law*. The NRC will promptly report suspected violations of Federal law to the appropriate Federal agency or suspected violations of State law to the appropriate State agency.

(o) *Procedures for processing of fingerprint checks*. (1) Licensees and certificate holders who have applied for § 73.19 authority, using an appropriate method listed in § 73.4, shall submit to the NRC's Division of Facilities and Security one (1) completed, legible standard fingerprint card (Form FD-258, ORIMDNRCOOOZ) or, where practicable, other fingerprint record for each individual requiring a firearms background check, to the NRC's Director, Division of Facilities and Security, Mail Stop T6-E46, ATTN: Criminal History Check. Copies of this form may be obtained by writing the Office of Information Services, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, by calling (301) 415-6157, or by e-mail to FORMS@nrc.gov. Guidance on what alternative formats, including electronic submissions, may be practicable are referenced in § 73.4.

(2) Licensees and certificate holders shall indicate on the fingerprint card or other fingerprint record that the purpose for this fingerprint check is the accomplishment of a firearms background check.

(3) Licensees and certificate holders shall establish procedures to ensure that the quality of the fingerprints taken results in minimizing the rejection rate of fingerprint cards or records due to illegible or incomplete information.

(4) The Commission will review fingerprints for firearms background checks for completeness. Any Form FD-258 or other fingerprint record containing omissions or evident errors will be returned to the licensee or certificate holder for corrections. The fee for processing fingerprint checks includes one (1) free re-submission if the initial submission is returned by the FBI because the fingerprint impressions cannot be classified. The one (1) free re-submission must have the FBI Transaction Control Number reflected on the re-submission. If additional submissions are necessary, they will be treated as an initial submittal and require a second payment of the processing fee. The payment of a new processing fee entitles the submitter to an additional free re-submittal, if necessary. Previously rejected submissions may not be included with the third submission because the submittal will be rejected automatically. Licensees and certificate holders may wish to consider using different methods for recording fingerprints for resubmissions, if difficulty occurs with obtaining a legible set of impressions.

(5)(i) Fees for the processing of fingerprint checks are due upon application. Licensees and certificate holders shall submit payment with the application for the processing of fingerprints, and payment must be made by corporate check, certified check, cashier's check, money order, or electronic payment, made payable to “U.S. NRC."[1] Combined payment for multiple applications is acceptable.

---

[1] For guidance on making electronic payments, contact the NRC’s Security Branch, Division of Facilities and Security, Office of Administration at (301) 415-7404.

(ii) The application fee is the sum of the user fee charged by the FBI for each fingerprint card or other fingerprint record submitted by the NRC on behalf of a licensee or certificate holder, and an administrative processing fee assessed by the NRC. The NRC processing fee covers administrative costs associated with NRC handling of licensee and certificate holder fingerprint submissions. The Commission publishes the amount of the fingerprint check application fee on the NRC's public Web site.[2] The Commission will directly notify licensees and certificate holders who are subject to this regulation of any fee changes.

(6) The Commission will forward to the submitting licensee or certificate holder all data received from the FBI as a result of the licensee's or certificate holder's application(s) for fingerprint background checks, including the FBI's fingerprint record.

(p) *Appeals and correction of erroneous system information*.

(1) Individuals who require a firearms background check under this section and who receive a "denied" NICS response or a "delayed" NICS response may not be assigned duties requiring access to covered weapons during the pendency of an appeal of the results of the check or during the pendency of providing and evaluating any necessary additional information to the FBI to resolve the "delayed" response, respectively.

(2) Licensees and certificate holders shall provide information on the FBI's procedures for appealing a "denied" response to the denied individual or on providing additional information to the FBI to resolve a "delayed" response.

(3) An individual who receives a "denied" or "delayed" NICS response to a firearms background check under this section may request the reason for the response from the FBI. The licensee or certificate holder shall provide to the individual who has received the "denied" or

[2] For information on the current fee amount, refer to the Electronic Submittals page at http://www.nrc.gov/site-help/eie.html and select the link for the Criminal History Program.

"delayed" response the unique NICS transaction number associated with the specific firearms background check.

(4) These requests for the reason for a "denied" or "delayed" NICS response must be made in writing, and must include the NICS transaction number. The request must be sent to the Federal Bureau of Investigation; NICS Section; Appeals Service Team, Module A-1; PO Box 4278; Clarksburg, WV 26302-9922. The FBI will provide the individual with the reasons for the "denied" response or "delayed" response. The FBI will also indicate whether additional information or documents are required to support an appeal or resolution, for example, where there is a claim that the record in question does not pertain to the individual who was denied.

(5) If the individual wishes to challenge the accuracy of the record upon which the "denied" or "delayed" response is based, or if the individual wishes to assert that his or her rights to possess or receive a firearm have been restored by lawful process, he or she may make application first to the FBI. The individual shall file an appeal of a “denied” response or file a request to resolve a "delayed" response within 45 calender days of the date the NRC forwards the results of the firearms background check to the licensee or certificate holder. The appeal or request must include appropriate documentation or record(s) establishing the legal and/or factual basis for the challenge. Any record or document of a court or other government entity or official furnished in support of an appeal must be certified by the court or other government entity or official as a true copy. The individual may supplement their initial appeal or request – subsequent to the 45 day filing deadline – with additional information as it becomes available, for example, where obtaining a true copy of a court transcript may take longer than 45 days. The individual should note in their appeal or request any information or records that are being obtained, but are not yet available.

(6) If the individual is notified that the FBI is unable to resolve the appeal, the individual may then apply for correction of the record directly to the agency from which the information

forming the basis of the denial was originated. If the individual is notified by the originating agency, that additional information or documents are required the individual may provide them to the originating agency. If the record is corrected as a result of the appeal to the originating agency, the individual may so notify the FBI and submit written proof of the correction.

(7) An individual who has satisfactorily appealed a "denied" response or resolved a "delayed" response may provide written consent to the FBI to maintain information about himself or herself in a Voluntary Appeal File (VAF) to be established by the FBI and checked by the NICS for the purpose of preventing the erroneous denial or extended delay by the NICS of any future NICS checks.

(8) Individuals appealing a "denied" response or resolving a “delayed” response are responsible for providing the FBI any additional information the FBI requires to resolve the “delayed” response.

11. Section 73.19 is added to read as follows:

§ 73.19 Authorization for preemption of firearms laws and use of enhanced weapons.

(a) *Purpose*. This section sets forth the requirements for licensees and certificate holders to obtain NRC approval to use the expanded authorities provided under section 161A of the Atomic Energy Act of 1954 (AEA), in protecting NRC-designated facilities, radioactive material, or other property. These authorities include “preemption authority” and “enhanced-weapons authority.”

(b) *General Requirements*. Licensees and certificate holders listed in paragraph (c) of this section may apply to the NRC, in accordance with the provisions of this section, to receive

stand-alone preemption authority or combined enhanced weapons authority and preemption authority.

(1) Preemption authority, as provided in section 161A of the AEA, means the authority of the Commission to permit licensees or certificate holders, or the designated security personnel of the licensee or certificate holder, to transfer, receive, possess, transport, import, or use one (1) or more category of standard and enhanced weapons, as defined in § 73.2, notwithstanding any local, State, or certain Federal firearms laws (including regulations).

(2) Enhanced weapons authority, as provided in section 161A of the AEA, means the authority of the Commission to permit licensees or certificate holders, or the designated security personnel of the licensee or certificate holder, to transfer, receive, possess, transport, import, and use one (1) or more category of enhanced weapons, as defined in § 73.2, notwithstanding any local, State, or certain Federal firearms laws (including regulations).

(3) Prior to receiving NRC approval of enhanced-weapons authority, the licensee or certificate holder must have applied for and received NRC approval for preemption authority, in accordance with this section or under Commission orders.

(4) Prior to granting either authority, the NRC must determine that the proposed use of this authority is necessary in the discharge of official duties by security personnel engaged in protecting –

(i) Facilities owned or operated by a licensee or certificate holder and designated by the Commission under paragraph (c) of this section, or

(ii) Radioactive material or other property that is owned or possessed by a licensee or certificate holder, or that is being transported to or from an NRC-regulated facility. Before granting such approval, the Commission must determined that the radioactive material or other property is of significance to the common defense and security or public health and safety and has designated such radioactive material or other property under paragraph (c) of this section.

(c) *Applicability*. (1) The following classes of licensees or certificate holders may apply for stand-alone preemption authority –

(i) Power reactor facilities; and

(ii) Facilities authorized to possess a formula quantity or greater of strategic special nuclear material with security plans subject to §§ 73.20, 73.45, and 73.46.

(2) The following classes of licensees or certificate holders may apply for combined enhanced-weapons authority and preemption authority –

(i) Power reactor facilities; and

(ii) Facilities authorized to possess a formula quantity or greater of strategic special nuclear material with security plans subject to §§ 73.20, 73.45, and 73.46.

(3) With respect to the possession and use of firearms by all other NRC licensees or certificate holders, the Commission's requirements in effect before **[effective date of final rule]** remain applicable, except to the extent those requirements are modified by Commission order or regulations applicable to such licensees and certificate holders.

(d) *Application for preemption authority*. (1) Licensees and certificate holders listed in paragraph (c) of this section may apply to the NRC for the preemption authority described in paragraph (b)(1) of this section. Licensees and certificate holders seeking such authority shall submit an application to the NRC in writing, in accordance with § 73.4, and indicate that the licensee or certificate holder is requesting preemption authority under section 161A of the AEA.

(2) Licensees and certificate holders who have applied for preemption authority under this section may begin firearms background checks under § 73.18 for their armed security personnel.

(3) Licensees and certificate holders who have applied for preemption authority under this section and who have satisfactorily completed firearms background checks for a sufficient number of security personnel (to implement their security plan while meeting security personnel

fatigue requirements of this chapter or Commission order) shall notify the NRC, in accordance with § 73.4, of their readiness to receive NRC approval of preemption authority and implement all the provisions of § 73.18.

(4) Based upon the licensee's or certificate holder's readiness notification and any discussions with the licensee or certificate holder, the NRC will document in writing to the licensee or certificate holder that the Commission has approved or disapproved the licensee's or certificate holder's application for preemption authority.

(e) *Application for enhanced-weapons authority*. (1) Licensees and certificate holders listed in paragraph (c)(2) of this section may apply to the NRC for enhanced-weapons authority described in paragraph (a)(2) of this section. Licensees and certificate holders applying for enhanced-weapons authority shall have also applied for preemption authority. Licensees and certificate holders may make these applications concurrently.

(2) Licensees and certificate holders seeking enhanced-weapons authority shall submit an application to the NRC, in accordance with § 73.4, indicating that the licensee or certificate holder is requesting enhanced-weapons authority under section 161A of the AEA. Licensees and certificate holders shall also include with their application -

(i) The additional information required by paragraph (f) of this section;

(ii) The date they applied to the NRC for preemption authority (if not concurrent with the application for enhanced weapons authority); and

(iii) If applicable, the date when the licensee or certificate holder received NRC approval of their application for preemption authority under this section or by Commission order.

(3) The NRC will document in writing to the licensee or certificate holder that the Commission has approved or disapproved the licensee's or certificate holder's application for enhanced-weapons authority. The NRC must approve, or have previously approved, a

licensee's or certificate holder's application for preemption authority under paragraph (d) of this section, or via Commission order, to approve the application for enhanced weapons authority.

(4) Licensees and certificate holders who have applied to the NRC for and received enhanced-weapons authority shall then apply to the U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) for a federal firearms license (FFL) and also register under the National Firearms Act (NFA) in accordance with ATF's regulations under 27 CFR parts 478 and 479 to obtain the enhanced weapons. Licensees and certificate holders shall include a copy of the NRC's written approval with their NFA registration application.

(f) *Application for enhanced-weapons authority additional information*. (1) Licensees and certificate holders applying to the Commission for enhanced-weapons authority under paragraph (e) of this section shall also submit to the NRC for prior review and written approval new, or revised, physical security plans, security personnel training and qualification plans, safeguards contingency plans, and safety assessments incorporating the use of the specific enhanced weapons the licensee or certificate holder intends to use. These plans and assessments must be specific to the facility, radioactive material, or other property being protected.

(2) In addition to other requirements set forth in this part, these plans and assessments must –

(i) For the physical security plan, identify the specific types or models, calibers, and numbers of enhanced weapons to be used;

(ii) For the training and qualification plan, address the training and qualification requirements to use these specific enhanced weapons; and

(iii) For the safeguards contingency plan, address how these enhanced and any standard weapons will be employed by the licensee's or certificate holder's security personnel in meeting the NRC-required protective strategy, including tactical approaches and maneuvers.

(iv) For the safety assessment –

(A) Assess any potential safety impact on the facility, radioactive material, or other property from the use of these enhanced weapons;

(B) Assess any potential safety impact on public or private facilities, public or private property, or on members of the public in areas outside of the site boundary from the use of these enhanced weapons; and

(C) Assess any potential safety impact on public or private facilities, public or private property, or on members of the public from the use of these enhanced weapons at training facilities intended for proficiency demonstration and qualification purposes.

(3) The licensee's or certificate holder's training and qualification plan on possessing, storing, maintaining, qualifying on, and using enhanced weapons must include information from applicable firearms standards developed by nationally-recognized firearms organizations or standard setting bodies or standards developed by Federal agencies, such as: the U.S. Department of Homeland Security's Federal Law Enforcement Training Center, the U.S. Department of Energy's National Training Center, and the U.S. Department of Defense.

(4) Licensees or certificate holders shall submit any new or revised plans and assessments for prior NRC review and written approval notwithstanding the provisions of §§ 50.54(p), 70.32(e), and 76.60 of this chapter which otherwise permit a license or certificate holder to make changes to such plans "that would not decrease their effectiveness" without prior NRC review.

(g) *Completion of training and qualification prior to use of enhanced weapons*. Licensees and certificate holders who have applied for and received enhanced-weapons authority under paragraph (e) of this section shall ensure security personnel complete required firearms training and qualification in accordance with the licensee's or certificate holder's NRC-approved training and qualification plan. Such training must be completed prior to security personnel's use of enhanced weapons to protect NRC-designated facilities, radioactive material,

or other property and must be documented in accordance with the requirements of the licensee's or certificate holder's training and qualification plan.

(h) *Use of enhanced weapons*. Requirements regarding the use of enhanced weapons by security personnel in the performance of their official duties are contained in §§ 73.46 and 73.55 and in appendices B and C of this part, as applicable.

(i) [Reserved].

(j) *Notification of adverse ATF findings or notices*. NRC licensees and certificate holders with an ATF federal firearms license (FFL) and/or enhanced weapons shall notify the NRC, in accordance with § 73.4, of instances involving any adverse ATF findings or ATF notices related to their FFL or such weapons.

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 **[date - 180 days - after the effective date of the final rule published in the *Federal Register*]**, each nuclear power reactor licensee, licensed under 10 CFR part 50, shall incorporate the revised requirements of this section through amendments to its Commission-approved Physical Security Plan, Training and Qualification Plan, and Safeguards Contingency Plan, referred to collectively as “approved security plans,” and shall submit the amended security plans to the Commission for review and approval.

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

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

(4) The licensee is responsible for maintaining the onsite physical protection program in accordance with Commission regulations and related Commission-directed orders through the implementation of the approved security plans and site implementing procedures.

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

(6) For licenses issued after [effective date of the final rule], licensees shall design construct, and equip the central alarm station and secondary alarm station to equivalent standards.

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

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

(b) General performance objective and requirements.

(1) The licensee shall establish and maintain a physical protection program, to include a security organization which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

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

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

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

(5) Upon the request of an authorized representative of the Commission, the licensee shall demonstrate the ability to meet Commission requirements through the implementation of the physical protection program, including the ability of armed and unarmed personnel to perform assigned duties and responsibilities required by the approved security plans and licensee procedures.

(6) The licensee shall establish and maintain a written performance evaluation program in accordance with appendix B and appendix C to this part, to demonstrate and assess the effectiveness of armed responders and armed security officers to perform their assigned duties and responsibilities to protect target sets described in paragraph (f) of this section and appendix C to this part, through implementation of the licensee protective strategy.

(7) The licensee shall establish, maintain, and follow an access authorization program in accordance with § 73.56.

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

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

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

(c) Security plans.

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

(i) How the physical protection program will prevent significant core damage and spent fuel sabotage through the establishment and maintenance of a security organization, the use of security equipment and technology, the training and qualification of security personnel, and the implementation of predetermined response plans and strategies; and

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

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

(3) Physical security plan.

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

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

(4) Training and qualification plan.

(i) The licensee shall establish, maintain, and follow a Commission-approved training and qualification plan, that describes how the criteria set forth in appendix B “General Criteria for Security Personnel,” to this part will be implemented.

(ii) The training and qualification plan must describe the process by which armed and unarmed security personnel, watchpersons, and other members of the security organization will be selected, trained, equipped, tested, qualified, and re-qualified to ensure that these individuals possess and maintain the knowledge, skills, and abilities required to carry out their assigned duties and responsibilities effectively.

(5) Safeguards contingency plan.

(i) The licensee shall establish, maintain, and implement a Commission-approved safeguards contingency plan that describes how the criteria set forth in section II of appendix C, "Licensee Safeguards Contingency Plans," to this part will be implemented.

(ii) The safeguards contingency plan must describe predetermined actions, plans, and strategies designed to intercept, challenge, delay, and neutralize threats up to and including the design basis threat of radiological sabotage.

(6) Implementing procedures.

(i) The licensee shall establish, maintain, and implement written procedures that document the structure of the security organization, detail the specific duties and responsibilities of each position, and implement Commission requirements through the approved security plans.

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

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

(iv) The licensee shall:

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

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

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

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

(d) Security organization.

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

(2) The security organization must include:

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

(ii) At least one member, onsite and available at all times, who has the authority to direct the activities of the security organization and who is assigned no other duties that would interfere

with this individual's ability to perform these duties in accordance with the approved security plans and licensee protective strategy.

(3) The licensee may not permit any individual to act as a member of the security organization unless the individual has been trained, equipped, and qualified to perform assigned duties and responsibilities in accordance with the requirements of appendix B to part 73 and the Commission-approved training and qualification plan.

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

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

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

(ii) The Commission may inspect, copy, retain, and remove all reports and documents required to be kept by Commission regulations, orders, or applicable license conditions whether the reports and documents are kept by the licensee or the contractor.

(iii) An individual may not be assigned to any position involving detection, assessment, or response to unauthorized activities unless that individual has satisfied the requirements of § 73.56.

(iv) An individual may not be assigned duties and responsibilities required to implement the approved security plans or licensee protective strategy unless that individual has been properly trained, equipped, and qualified to perform their assigned duties and responsibilities in

accordance with appendix B to part 73 and the Commission-approved training and qualification plan.

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

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

(e) Physical barriers. Based upon the licensee's protective strategy, analyses, and site conditions that affect the use and placement of physical barriers, the licensee shall install and maintain physical barriers that are designed and constructed as necessary to deter, delay, and prevent the introduction of unauthorized personnel, vehicles, or materials into areas for which access must be controlled or restricted.

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

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

(3) Physical barriers must:

(i) Clearly delineate the boundaries of the area(s) for which the physical barrier provides protection or a function, such as protected and vital area boundaries and stand-off distance.

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

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

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

(4) Owner controlled area. The licensee shall establish and maintain physical barriers in the owner controlled area to deter, delay, or prevent unauthorized access, facilitate the early detection of unauthorized activities, and control approach routes to the facility.

(5) Isolation zone.

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

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

(B) Equipped with intrusion detection equipment capable of detecting both attempted and actual penetration of the protected area perimeter barrier and assessment equipment capable of facilitating timely evaluation of the detected unauthorized activities before completed penetration of the protected area perimeter barrier.

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

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

(6) Protected area.

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

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

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

(iv) Where building walls, roofs, or penetrations comprise a portion of the protected area perimeter barrier, an isolation zone is not necessary, provided that the detection, assessment, observation, monitoring, and surveillance requirements of this section are met, appropriately designed and constructed barriers are installed, and the area is described in the approved security plans.

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

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

(7) Vital areas.

(i) Vital equipment must be located only within vital areas, which in turn must be located within protected areas so that access to vital equipment requires passage through at least two physical barriers designed and constructed to perform the required function, except as otherwise approved by the Commission in accordance with paragraph (f)(3) of this section.

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

(iii) The reactor control room, the spent fuel pool, secondary power supply systems for intrusion detection and assessment equipment, non-portable communications equipment, and the central alarm station, must be provided protection equivalent to vital equipment located within a vital area.

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

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

(vi) Unoccupied vital areas must be locked.

(8) Vehicle barrier system. The licensee must:

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

(ii) Limit and control all vehicle approach routes.

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

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

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

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

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

(9) Waterways.

(i) The licensee shall control waterway approach routes or proximity to any area from which a waterborne vehicle, its personnel, or its contents could disable the personnel, equipment, or systems necessary to meet the performance objective and requirements described in paragraph (b) of this section.

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

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

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

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

(f) Target sets.

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

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

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

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

(g) Access control.

(1) The licensee shall:

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

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

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

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

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

(vi) Isolate the individual responsible for the last access control function (controlling admission to the protected area) within a bullet-resisting structure to assure the ability to respond or to summon assistance in response to unauthorized activities.

(vii) In response to specific threat and security information, implement a two-person (line-of-sight) rule for all personnel in vital areas so that no one individual is permitted unescorted access to vital areas. Under these conditions, the licensee shall implement measures to verify that the two person rule has been met when a vital area is accessed.

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

(i) Confirm the identity of individuals.

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

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

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

(3) Access control points must be:

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

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

(4) Emergency conditions.

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

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

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

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

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

(iii) The licensee shall ensure that restrictions for site access and egress during emergency conditions are coordinated with responses by offsite emergency support agencies identified in the site emergency plans.

(5) Vehicles.

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

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

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

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

(6) Access control devices.

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

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

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

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

(ii) Keys, locks, combinations, and passwords. All keys, locks, combinations, passwords, and related access control devices used to control access to protected areas, vital areas, security systems, and safeguards information must be controlled and accounted for to reduce the probability of compromise. The licensee shall:

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

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

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

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

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

(7) Visitors.

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

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

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

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

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

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

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

(A) Non-employee, no escort required.

(B) Areas to which access is authorized.

(C) The period for which access is authorized.

(D) The individual's employer.

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

(8) Escorts. The licensee shall ensure that all escorts are trained in accordance with appendix B to this part, the approved training and qualification plan, and licensee policies and procedures.

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

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

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

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

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

(h) Search programs.

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

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

(ii) The search requirements for unauthorized firearms, explosives, incendiary devices, or other unauthorized materials and devices must be accomplished through the use of

equipment capable of detecting these unauthorized items and through visual and hands-on physical searches, as needed to ensure all items are identified before granting access.

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

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

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

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

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

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

(5) Vehicle search procedures must be performed by at least two (2) properly trained and equipped security personnel, at least one of whom is positioned to observe the search process and provide a timely response to unauthorized activities if necessary.

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

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

(8) Exceptions to the search requirements of this section must be submitted to the Commission for prior review and approval and must be identified in the approved security plans.

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

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

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

(i) Detection and assessment systems.

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

(2) Intrusion detection equipment must annunciate, and video assessment equipment images shall display, concurrently in at least two continuously staffed onsite alarm stations, at least one of which must be protected in accordance with the requirements of paragraphs (e)(6)(v), (e)(7)(iii), and (i)(8)(ii) of this section.

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

(i) Are concurrently notified of the alarm annunciation.

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

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

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

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

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

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

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

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

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

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

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

(iv) Provide visual and audible alarm annunciation and concurrent video assessment capability to both alarm stations in a manner that ensures timely recognition, acknowledgment and response by each alarm station operator in accordance with written response procedures.

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

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

(8) Alarm stations.

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

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

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

(iv) The licensee shall assess and respond to all alarms and other indications of unauthorized activities in accordance with the approved security plans and implementing procedures.

(v) The licensee's implementing procedures must ensure that both alarm station operators are knowledgeable of all alarm annunciations, assessments, and final disposition of all alarms, to include but not limited to a prohibition from changing the status of a detection point or deactivating a locking or access control device at a protected or vital area portal, without the knowledge and concurrence of the other alarm station operator.

(9) Surveillance, observation, and monitoring.

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

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

(A) Continual surveillance, observation, and monitoring responsibilities must be performed by security personnel during routine patrols or by other trained and equipped personnel designated as a component of the protective strategy.

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

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

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

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

(C) Security personnel shall be trained to recognize indications of tampering as necessary to perform assigned duties and responsibilities as they relate to safety and security systems and equipment.

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

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

(10) Video technology.

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

(ii) Video technology must be:

(A) Displayed concurrently at both alarm stations.

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

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

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

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

(11) Illumination.

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

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

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

(j) Communication requirements.

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

(2) Individuals assigned to each alarm station shall be capable of calling for assistance in accordance with the approved security plans, licensee integrated response plan, and licensee procedures.

(3) Each on-duty security officer, watchperson, vehicle escort, and armed response force member shall be capable of maintaining continuous communication with an individual in each alarm station.

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

(i) Conventional telephone service.

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

(iii) A system for communication with all control rooms, on-duty operations personnel, escorts, local, state, and Federal law enforcement agencies, and all other personnel necessary to coordinate both onsite and offsite responses.

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

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

(k) Response requirements.

(1) Personnel and equipment.

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

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

(iii) The licensee shall describe in the approved security plans, all firearms and equipment to be possessed by and readily available to, armed personnel to implement the protective strategy and carry out all assigned duties and responsibilities. This description must

include the general distribution and assignment of firearms, ammunition, body armor, and other equipment used.

(iv) The licensee shall ensure that all firearms, ammunition, and equipment required by the protective strategy are in sufficient supply, are in working condition, and are readily available for use in accordance with the licensee protective strategy and predetermined time lines.

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

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

(3) The licensee shall provide an armed response team consisting of both armed responders and armed security officers to carry out response duties, within predetermined time lines.

(i) Armed responders.

(A) The licensee shall determine the minimum number of armed responders necessary to protect against the design basis threat described in § 73.1(a), subject to Commission approval, and shall document this number in the approved security plans.

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

(ii) Armed security officers.

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

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

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

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

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

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

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

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

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

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

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

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

(8) The licensee shall document and maintain current agreements with local, state, and Federal law enforcement agencies, to include estimated response times and capabilities.

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

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

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

(3) Administrative controls.

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

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

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

(A) Inspect unirradiated MOX fuel assemblies for damage.

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

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

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

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

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

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

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

(4) Physical controls.

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

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

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

(iv) Locks, keys, and any other access control device used to secure equipment and power sources required for the movement of unirradiated MOX fuel assemblies or openings to

areas containing unirradiated MOX fuel assemblies must be controlled by the security organization.

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

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

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

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

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

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

(m) Digital computer and communication networks.

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

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

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

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

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

(3) Policies, requirements, and procedures.

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

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

(4) Incident response and recovery.

(i) The licensee shall implement a cyber-security incident response and recovery plan to minimize the adverse impact of a cyber-security incident on safety, security, or emergency preparedness systems.

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

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

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

(6) Configuration and control management program. The licensee shall implement a configuration and control management program, to include cyber risk analysis, to ensure that modifications to computer system designs, access control measures, configuration, operational integrity, and management process do not adversely impact facility safety, security, and emergency preparedness systems before implementation of those modifications.

(7) Cyber-security awareness and training.

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

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

(n) Security program reviews and audits.

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

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

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

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

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

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

(3) The licensee shall periodically review the approved security plans, the integrated response plan, the licensee protective strategy, and licensee implementing procedures to evaluate their effectiveness and potential impact on plant and personnel safety.

(4) The licensee shall periodically evaluate the cyber-security program for effectiveness and shall update the cyber-security program as needed to ensure protection against changes to internal and external threats.

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

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

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

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

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

(o) Maintenance, testing, and calibration.

(1) The licensee shall:

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

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

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

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

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

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

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

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

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

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

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

(p) Compensatory measures.

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

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

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

(q) Suspension of safeguards measures.

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

(i) In accordance with §§ 50.54(x) and 50.54(y) of this chapter, the licensee may suspend any safeguards measures pursuant to this section in an emergency when this action is immediately needed to protect the public health and safety and no action consistent with license conditions and technical specifications that can provide adequate or equivalent protection is immediately apparent. This suspension of safeguards measures must be approved as a minimum by a licensed senior operator prior to taking this action.

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

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

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

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

(r) Records.

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

(2) The licensee shall maintain all records required to be kept by Commission regulations, orders, or license conditions, as a record until the Commission terminates the license for which the records were developed and shall maintain superseded portions of these

records for at least three (3) years after the record is superseded, unless otherwise specified by the Commission.

(s) Safety/security interface. In accordance with the requirements of § 73.58, the licensee shall develop and implement a process to inform and coordinate safety and security activities to ensure that these activities do not adversely affect the capabilities of the security organization to satisfy the requirements of this section, or overall plant safety.

(t) Alternative measures.

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

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

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

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

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

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

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

(ii) Based on comparison of the costs of the alternative measures to the costs of meeting the Commission's requirements using the essential elements of 10 CFR 50.109, the costs of fully meeting the Commission's requirements are not justified by the protection that would be provided.

13. Section 73.56 is revised to read as follows:

§ 73.56 Personnel access authorization requirements for nuclear power plants.

(a) Introduction. (1) By **[date - 180 days - after the effective date of the final rule published in the *Federal Register*]**, each nuclear power reactor licensee, licensed under 10 CFR part 50, shall incorporate the revised requirements of this section through amendments to its Commission-approved access authorization program and shall submit the amended program to the Commission for review and approval.

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

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

(4) The licensee is responsible to the Commission for maintaining the authorization program in accordance with Commission regulations and related Commission-directed orders through the implementation of the approved program and site implementing procedures.

(5) Applicants for an operating license under the provisions of part 50 of this chapter, or holders of a combined license under the provisions of part 52 of this chapter, shall satisfy the requirements of this section upon receipt of an operating license or upon notice of the Commission's finding under § 52.103(g) of this chapter.

(6) Contractors and vendors (C/Vs) who implement authorization programs or program elements shall develop, implement, and maintain authorization programs or program elements that meet the requirements of this section, to the extent that the licensees and applicants specified in paragraphs (a)(1) and (a)(5) of this section rely upon those C/V authorization programs or program elements to meet the requirements of this section. In any case, only a licensee or applicant shall grant or permit an individual to maintain unescorted access to nuclear power plant protected and vital areas.

(b) Individuals who are subject to an authorization program.

(1) The following individuals shall be subject to an authorization program:

(i) Any individual to whom a licensee or applicant grants unescorted access to nuclear power plant protected and vital areas.

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

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

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

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

(c) General performance objective. Access authorization programs must provide high assurance that the individuals who are specified in paragraph (b)(1) of this section, and, if applicable, (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 unescorted access authorization to an individual, the licensees, applicants, and C/Vs specified in paragraph (a) of this section shall ensure that the individual has been subject to a background investigation. The background investigation must include, but is not limited to, the following elements:

(1) Informed consent. The licensees, applicants, and C/Vs specified in paragraph (a) of this section may not initiate any element of a background investigation without the knowledge and written consent of the subject individual. Licensees, applicants, and C/Vs shall inform the individual of his or her right to review information collected to assure its accuracy and provide the individual with an opportunity to correct any inaccurate or incomplete information that is developed by licensees, applicants, and C/Vs about the individual.

(i) The subject individual may withdraw his or her consent at any time. The licensee, applicant, or C/V to whom the individual has applied for unescorted access authorization shall inform the individual that —

(A) Withdrawal of his or her consent will withdraw the individual's current application for access authorization under the licensee's, applicant's, or C/V's authorization program; and

(B) Other licensees, applicants, and C/Vs will have access to information documenting the withdrawal through the information-sharing mechanism required under paragraph (o)(6) of this section.

(ii) If an individual withdraws his or her consent, the licensees, applicants, and C/Vs specified in paragraph (a) of this section 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. In the information-sharing mechanism required under paragraph (o)(6) of this

section, the licensee, applicant, or C/V shall record the individual's application for unescorted access authorization; his or her withdrawal of consent for the background investigation; the reason given by the individual for the withdrawal, if any; and any pertinent information collected from the background investigation elements that were completed.

(iii) The licensees, applicants, and C/Vs specified in paragraph (a) of this section shall inform, in writing, any individual who is applying for unescorted access authorization that the following actions related to providing and sharing the personal information under this section are sufficient cause for denial or unfavorable termination of unescorted access authorization:

(A) Refusal to provide written 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 authorization;

(C) Refusal to provide written consent for the sharing of personal information with other licensees, applicants, or C/Vs required under paragraph (d)(4)(v) of this section; and

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

(2) Personal history disclosure.

(i) Any individual who is applying for unescorted access authorization shall disclose the personal history information that is required by the licensee's, applicant's, or C/V's authorization program and 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 C/Vs may not require an individual to disclose an administrative withdrawal of unescorted access authorization under the requirements of paragraphs (g), (h)(7), or (i)(1)(v) of this section, if the individual's unescorted access

authorization was not subsequently denied or terminated unfavorably by a licensee, applicant, or C/V.

(3) Verification of true identity. Licensees, applicants, and C/Vs shall verify the true identity of an individual who is applying for 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 C/Vs shall validate the social security number that the individual has provided, and, in the case of foreign nationals, the alien registration number that the individual provides. In addition, licensees, applicants, and C/Vs shall also determine whether the results of the fingerprinting required under § 73.21 confirm the individual's claimed identity, if such results are available.

(4) Employment history evaluation. Licensees, applicants, and C/Vs shall ensure that an employment history evaluation has been completed, by questioning the individual's present and former employers, and by determining the activities of individuals while unemployed.

(i) For the claimed employment period, the employment history evaluation must ascertain the reason for 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 licensee, applicant, or C/V who is conducting the employment history evaluation shall request a characterization of service, reason for separation, and any disciplinary actions that could affect a trustworthiness and reliability determination.

(iii) Periods of self-employment or unemployment may be verified by any reasonable method. If education is claimed in lieu of employment, the licensee, applicant, or C/V shall request information that could reflect on the individual's trustworthiness and reliability and, at a minimum, verify that the individual was actively participating in the educational process during the claimed period.

(iv) If a company, previous employer, or educational institution to whom the licensee, applicant, or C/V has directed a request for information refuses to provide information or indicates an inability or unwillingness to provide information within 3 business days of the request, the licensee, applicant, or C/V shall document this refusal, inability, or unwillingness in the licensee's, applicant's, or C/V's record of the investigation, and obtain a confirmation of employment or educational enrollment and attendance from at least one alternate source, with questions answered to the best of the alternate source's ability. This alternate source may not have been previously used by the licensee, applicant, or C/V to obtain information about the individual's character and reputation. If the licensee, applicant, or C/V uses an alternate source because employment information is not forthcoming within 3 business days of the request, the licensee, applicant, or C/V need not delay granting unescorted access authorization to wait for any employer response, but shall evaluate and document the response if it is received.

(v) When any licensee, applicant, or C/V specified in paragraph (a) of this section is legitimately seeking the information required for an unescorted access authorization decision under this section and has obtained a signed release from the subject individual authorizing the disclosure of such information, a licensee, applicant, or C/V who is subject to this section shall disclose whether the subject individual's unescorted access authorization was denied or terminated unfavorably. The licensee, applicant, or C/V who receives the request for information shall make available the information upon which the denial or unfavorable termination of unescorted access authorization was based.

(vi) In conducting an employment history evaluation, the licensee, applicant, or C/V may obtain information and documents by electronic means, including, but not limited to, telephone, facsimile, or email. The licensee, applicant, or C/V shall make a record of the contents of the telephone call and shall retain that record, and any documents or files obtained electronically, in accordance with paragraph (o) of this section.

(5) Credit history evaluation. The licensees, applicants, and C/Vs specified in paragraph (a) of this section shall ensure that the full credit history of any individual who is applying for unescorted access authorization has been evaluated. A full credit history evaluation must include, but would not be 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.

(6) Character and reputation. The licensees, applicants, and C/Vs specified in paragraph (a) of this section shall ascertain the character and reputation of an individual who has applied for 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, applicant's, or C/V's reviewing official shall evaluate the entire criminal history record of an individual who is applying for unescorted access authorization to assist in determining whether the individual has a record of criminal activity that may adversely impact his or her trustworthiness and reliability. The criminal history record must be obtained in accordance with the requirements of § 73.57.

(e) Psychological assessment. In order to assist in determining an individual's trustworthiness and reliability, the licensees, applicants, and C/Vs specified in paragraph (a) of this section shall ensure that a psychological assessment has been completed of the individual who is applying for unescorted access authorization. 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 clinical psychologist or psychiatrist 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 implications for an individual's trustworthiness and reliability. Predetermined thresholds must be applied in interpreting the results of the psychological test, to determine whether an individual shall be interviewed by a psychiatrist or licensed clinical psychologist under paragraph (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 licensee's or applicant's Physical Security Plan requires a clinical interview based on job assignments.

(5) If, in the course of conducting the psychological assessment, the licensed clinical psychologist or psychiatrist identifies indications of, or information related to, a medical condition that could adversely impact the individual's fitness for duty or trustworthiness and reliability, the psychologist or psychiatrist shall inform the reviewing official, who shall ensure that an appropriate evaluation of the possible medical condition is conducted under the requirements of part 26 of this chapter.

(f) Behavioral observation. Access authorization programs must include a behavioral observation element that is designed to detect behaviors or activities that may constitute an unreasonable risk to the health and safety of the public and common defense and security, including a potential threat to commit radiological sabotage.

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

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

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

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

(iii) Individuals shall demonstrate the successful completion of behavioral observation training by passing a comprehensive examination that addresses the knowledge and abilities necessary to detect behavior or activities that have the potential to constitute an unreasonable risk to the health and safety of the public and common defense and security, including a

potential threat to commit radiological sabotage. Remedial training and re-testing are required for individuals who fail to satisfactorily complete the examination.

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

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

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

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

(1) Accepting unescorted access authorization from other authorization programs. Licensees, applicants, and C/Vs who are seeking to grant unescorted access authorization to an individual who is subject to another authorization program that complies with this section may rely on the program elements completed by the transferring authorization program to satisfy the requirements of this section. An individual may maintain his or her unescorted access authorization if he or she continues to be subject to either the receiving licensee's, applicant's, or

C/V's authorization program or the transferring licensee's, applicant's, or C/V's authorization program, or a combination of elements from both programs that collectively satisfy the requirements of this section. The receiving authorization program shall ensure that the program elements maintained by the transferring program remain current.

(2) Information sharing. To meet the requirements of this section, licensees, applicants, and C/Vs may rely upon the information that other licensees, applicants, and C/Vs who are subject to this section have gathered about individuals who have previously applied for unescorted access authorization and developed about individuals during periods in which the individuals maintained unescorted access authorization.

(3) Requirements applicable to all unescorted access authorization categories. Before granting unescorted access authorization to individuals in any category, including individuals whose unescorted access authorization has been interrupted for a period of 30 or fewer days, the licensee, applicant, or C/V shall ensure that —

(i) The individual's written consent to conduct a background investigation, if necessary, has been obtained and the individual's true identity has been verified, in accordance with paragraphs (d)(2) and (d)(3) of this section, respectively;

(ii) A credit history evaluation or re-evaluation has been completed in accordance with the requirements of paragraphs (d)(5) or (i)(1)(v) of this section, as applicable;

(iii) The individual's character and reputation have been ascertained, in accordance with paragraph (d)(6) of this section;

(iv) The individual's criminal history record has been obtained and reviewed or updated, in accordance with paragraphs (d)(7) and (i)(1)(v) of this section, as applicable;

(v) A psychological assessment or reassessment of the individual has been completed in accordance with the requirements of paragraphs (e) or (i)(1)(v) of this section, as applicable;

(vi) The individual has successfully completed the initial or refresher, as applicable, behavioral observation training that is required under paragraph (f) of this section; and

(vii) The individual has been informed, in writing, of his or her arrest-reporting responsibilities under paragraph (g) of this section.

(4) Interruptions in unescorted access authorization. For individuals who have previously held unescorted access authorization under this section but whose unescorted access authorization has since been terminated under favorable conditions, the licensee, applicant, or C/V shall implement the requirements in this paragraph for initial unescorted access authorization in paragraph (h)(5) of this section, updated unescorted access authorization in paragraph (h)(6) of this section, or reinstatement of unescorted access authorization in paragraph (h)(7) of this section, based upon the total number of days that the individual's unescorted access authorization has been interrupted, to include the day after the individual's last period of unescorted access authorization was terminated and the intervening days until the day upon which the licensee, applicant, or C/V grants unescorted access authorization to the individual. If potentially disqualifying information is disclosed or discovered about an individual, licensees, applicants, and C/V's shall take additional actions, as specified in the licensee's or applicant's physical security plan, in order to grant or maintain the individual's unescorted access authorization.

(5) Initial unescorted access authorization. Before granting unescorted access authorization to an individual who has never held unescorted access authorization under this section or whose unescorted access authorization has been interrupted for a period of 3 years or more and whose last period of unescorted access authorization was terminated under favorable conditions, the licensee, applicant, or C/V shall ensure that an employment history evaluation has been completed in accordance with paragraph (d)(4) of this section. The period of the employment history that the individual shall disclose, and the licensee, applicant, or C/V shall

evaluate, must be the past 3 years or since the individual's eighteenth birthday, whichever is shorter. For the 1-year period immediately preceding the date upon which the individual applies for unescorted access authorization, the licensee, applicant, or C/V 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 C/V 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, if the individual claims employment during the given calendar month.

(6) Updated unescorted access authorization. Before granting unescorted access authorization to an individual whose unescorted access authorization has been interrupted for more than 365 days but fewer than 3 years and whose last period of unescorted access authorization was terminated under favorable conditions, the licensee, applicant, or C/V shall ensure that an employment history evaluation has been completed in accordance with paragraph (d)(4) of this section. The period of the employment history that the individual shall disclose, and the licensee, applicant, or C/V shall evaluate, must be the period since unescorted access authorization was last terminated, up to and including the day the applicant applies for updated unescorted access authorization. For the 1-year period immediately preceding the date upon which the individual applies for updated unescorted access authorization, the licensee, applicant, or C/V shall ensure that the employment history evaluation is conducted with every employer, regardless of the length of employment. For the remaining period since unescorted access authorization was last terminated, the licensee, applicant, or C/V 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, if the individual claims employment during the given calendar month.

(7) Reinstatement of unescorted access authorization (31 to 365 days). In order to grant authorization to an individual whose unescorted access authorization has been interrupted for a period of more than 30 days but no more than 365 days and whose last period of unescorted access authorization was terminated under favorable conditions, the licensee, applicant, or C/V shall ensure that an employment history evaluation has been completed in accordance with the requirements of paragraph (d)(4) of this section within 5 business days of reinstating unescorted access authorization. The period of the employment history that the individual shall disclose, and the licensee, applicant, or C/V shall evaluate, must be the period since the individual's unescorted access authorization was terminated, up to and including the day the applicant applies for reinstatement of unescorted access authorization. The licensee, applicant, or C/V 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, if the individual claims employment during a given calendar month. If the employment history evaluation is not completed within 5 business days due to circumstances that are outside of the licensee's, applicant's, or C/V's control and the licensee, applicant, or C/V is not aware of any potentially disqualifying information regarding the individual within the past 5 years, the licensee, applicant, or C/V may maintain the individual's unescorted access authorization for an additional 5 business days. If the employment history evaluation is not completed within 10 business days of reinstating unescorted access authorization, the licensee, applicant, or C/V shall administratively withdraw the individual's unescorted access authorization until the employment history evaluation is completed.

(8) Determination basis. The licensee's, applicant's, or C/V's reviewing official shall determine whether to grant, deny, unfavorably terminate, or maintain or amend an individual's unescorted access authorization status, based on an evaluation of all pertinent information that has been gathered about the individual as a result of any application for unescorted access

authorization or developed during or following in any period during which the individual maintained unescorted access authorization. The licensee's, applicant's, or C/V's reviewing official may not determine whether to grant unescorted access authorization to an individual or maintain an individual's unescorted access authorization until all of the required information has been provided to the reviewing official and he or she determines that the accumulated information supports a positive finding of trustworthiness and reliability.

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

(10) Access prohibited. Licensees and applicants may not permit an individual, who is identified as having an access-denied status in the information-sharing mechanism required under paragraph (o)(6) of this section, or has an access authorization status other than favorably terminated, to enter any nuclear power plant protected area 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 if, upon evaluation, the reviewing official determines that such access is warranted. Licensees and applicants shall develop reinstatement review procedures for assessing individuals who have been in an access-denied status.

(i) Maintaining access authorization.

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

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

(ii) The individual successfully completes behavioral observation refresher training or testing on the nominal 12-month frequency required in (f)(2)(ii) of this section;

(iii) The individual complies with the licensee's, applicant's, or C/V's authorization program policies and procedures to which he or she is subject, including the arrest-reporting responsibility specified in paragraph (g) of this section;

(iv) The individual is subject to a supervisory interview at a nominal 12-month frequency, conducted in accordance with the requirements of the licensee's or applicant's Physical Security Plan; and

(v) The licensee, applicant, or C/V determines that the individual continues to be trustworthy and reliable. This determination must be made as follows:

(A) The licensee, applicant, or C/V shall complete a criminal history update, credit history re-evaluation, and psychological re-assessment of the individual within 5 years of the date on which these elements were last completed, or more frequently, based on job assignment;

(B) The reviewing official shall complete an evaluation of the information obtained from the criminal history update, credit history re-evaluation, psychological re-assessment, and the supervisory interview required under paragraph (i)(1)(iv) of this section within 30 calendar days of initiating any one of these elements;

(C) The results of the criminal history update, credit history re-evaluation, psychological re-assessment, and the supervisory interview required under paragraph (i)(1)(iv) of this section must support a positive determination of the individual's continued trustworthiness and reliability; and

(D) If the criminal history update, credit history re-evaluation, psychological re-assessment, and supervisory review have not been completed and the information evaluated by the reviewing official within 5 years of the initial completion of these elements or the most recent update, re-evaluation, and re-assessment under this paragraph, or within the time period

specified in the licensee's or applicant's Physical Security Plans, the licensee, applicant, or C/V shall administratively withdraw the individual's unescorted access authorization until these requirements have been met.

(2) If an individual who has unescorted access authorization is not subject to an authorization program that meets the requirements of this part for more than 30 continuous days, then the licensee, applicant, or C/V shall terminate the individual's unescorted access authorization and the individual shall meet the requirements in this section, as applicable, to regain unescorted access authorization.

(j) Access to vital areas. Each licensee and applicant who is subject to this section shall establish, implement, and maintain a list of individuals who are authorized to have unescorted access to specific nuclear power plant vital areas to assist in limiting access to those vital areas during non-emergency conditions. The list must include only those individuals who require 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 authorization program personnel. Licensees, applicants, and C/Vs shall ensure that any individuals who collect, process, or have access to personal information that is used to make unescorted access authorization determinations under this section have been determined to be trustworthy and reliable.

(1) Background screeners. Licensees, applicants, and C/Vs 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 authorization determinations shall ensure that a

background check of such individuals has been completed and determines that such individuals are trustworthy and reliable. At a minimum, the following checks are required:

(i) Verification of the individual's identity;

(ii) A local criminal history review and evaluation from the State of the individual's permanent residence;

(iii) A credit history review and evaluation;

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

(v) An evaluation of character and reputation.

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

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

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

(l) Review procedures. Each licensee, applicant, and C/V who is implementing an authorization program under this section shall include a procedure for the review, at the request of the affected individual, of a denial or unfavorable termination of unescorted access

authorization. The procedure must require that the individual is informed of the grounds for the denial or unfavorable termination and allow the individual an opportunity to provide additional relevant information, and provide an opportunity for an objective review of the information on which the denial or unfavorable termination of unescorted access authorization was based. The procedure may be an impartial and independent internal management review. Licensees and applicants may not grant or permit the individual to maintain unescorted access authorization during the review process.

(m) Protection of information. Each licensee, applicant, or C/V who is subject to this section who collects personal information about an individual for the purpose of complying with this section, shall establish and maintain a system of files and procedures to protect the personal information.

(1) Licensees, applicants, and C/Vs shall obtain a signed consent from the subject individual that authorizes the disclosure of the personal information collected and maintained under this section before disclosing the personal 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 C/V'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 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; and

(vii) Other persons pursuant to court order.

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

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

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

(5) Licensees, applicants, and C/Vs who collect and maintain personal information under this section, and any individual or organization who collects and maintains personal information on behalf of a licensee, applicant, or C/V, shall establish, implement, and maintain a system and procedures for the secure storage and handling of the personal information collected.

(6) This paragraph does not authorize the licensee, applicant, or C/V to withhold evidence of criminal conduct from law enforcement officials.

(n) Audits and corrective action. Each licensee and applicant who is subject to this section shall be responsible for the continuing effectiveness of the authorization program, including authorization program elements that are provided by C/Vs, and the authorization programs of any C/Vs that are accepted by the licensee and applicant. Each licensee, applicant,

and C/V who is subject to this section shall ensure that authorization programs and program elements are audited to confirm compliance with the requirements of this section and that comprehensive actions are taken to correct any non-conformance that is identified.

(1) Each licensee, applicant, and C/V who is subject to this section shall ensure that their entire authorization program is audited as needed, but no less frequently than nominally every 24 months. Licensees, applicants, and C/Vs 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) Authorization program services that are provided to a licensee, or applicant, by C/V 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 on a nominal 12-month frequency. In addition, any authorization program services that are provided to C/Vs by subcontractor personnel who are off site or are not under the direct daily supervision or observation of the C/V's personnel must be audited on a nominal 12-month frequency.

(3) Licensees' and applicants' contracts with C/Vs must reserve the right to audit the C/V and the C/V's subcontractors providing 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) Licensees' and applicants' contracts with C/Vs, and a C/V's contracts with subcontractors, must also require that the licensee or applicant shall be provided with, or permitted access to, copies of any documents and take away any documents that may be needed to assure that the C/V 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 authorization program or program element(s), as appropriate. At least one member of the audit team shall be a person who is knowledgeable of and practiced with meeting authorization program performance objectives and requirements. The individuals performing the audit of the authorization program or program element(s) 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.

(6) The result of the audits, along with any recommendations, must be documented and reported to senior corporate and site management. Each audit report must identify conditions that are adverse to the proper performance of the authorization program, the cause of the condition(s), and, when appropriate, recommended corrective actions, and corrective actions taken. The licensee, applicant, or C/V shall review the audit findings and take any additional corrective actions, to include re-auditing of the deficient areas where indicated, to preclude, within reason, repetition of the condition. The resolution of the audit findings and corrective actions must be documented.

(7) Licensees and applicants may jointly conduct audits, or may accept audits of C/Vs that were conducted by other licensees and applicants who are subject to this section, if the audit addresses the services obtained from the C/V by each of the sharing licensees and applicants. C/Vs may jointly conduct audits, or may accept audits of its subcontractors that were conducted by other licensees, applicants, and C/Vs who are subject to this section, if the audit addresses the services obtained from the subcontractor by each of the sharing licensees, applicants, and C/Vs.

(i) Licensees, applicants, and C/Vs 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 C/V 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 C/V for the same period of time. Sharing C/Vs need not re-audit the same subcontractor for the same period of time.

(iii) Each sharing licensee, applicant, and C/V shall maintain a copy of the shared audit, including findings, recommendations, and corrective actions.

(o) Records. Each licensee, applicant, and C/V who is subject to this section 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) All 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) Each licensee, applicant, and C/V who is subject to this section shall retain the following records for at least 5 years after the licensee, applicant, or C/V terminates or denies an individual's unescorted access authorization or until the completion of all related legal proceedings, whichever is later:

(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 authorization;

(ii) Records pertaining to denial or unfavorable termination of unescorted access authorization and related management actions; and

(iii) Documentation of the granting and termination of unescorted access authorization.

(3) Each licensee, applicant, and C/V who is subject to this section shall retain the following records for at least 3 years or until the completion of all related legal 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 C/Vs shall retain written agreements for the provision of services under this section for the life of the agreement or until completion of all legal proceedings related to a denial or unfavorable termination of unescorted access authorization that involved those services, whichever is later.

(5) Licensees, applicants, and C/Vs shall retain records of the background checks, and psychological assessments of 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 C/V, or until the completion of any legal proceedings relating to the actions of such authorization program personnel, whichever is later.

(6) Licensees, applicants, and C/Vs shall ensure that the information about individuals who have applied for unescorted access authorization, which is specified in the licensee's or applicant's Physical Security Plan, is recorded and retained in an information-sharing mechanism that is established and administered by the licensees, applicants, and C/Vs who are subject to his section. Licensees, applicants, and C/Vs shall ensure that only correct and complete information is included in the information-sharing mechanism. If, for any reason, the

shared information used for determining an individual's trustworthiness and reliability changes or new information is developed about the individual, licensees, applicants, and C/Vs shall correct or augment the shared information contained in the information-sharing mechanism. If the changed or developed information has implications for adversely affecting an individual's trustworthiness and reliability, the licensee, applicant, or C/V who has discovered the incorrect information, or develops new information, shall inform the reviewing official of any authorization program under which the individual is maintaining unescorted access authorization of the updated information on the day of discovery. The reviewing official shall evaluate the information and take appropriate actions, which may include denial or unfavorable termination of the individual's unescorted access authorization. If, for any reason, the information-sharing mechanism is unavailable and a notification of changes or updated information is required, licensees, applicants, and C/Vs shall take manual actions to ensure that the information is shared, and update the records in the information-sharing mechanism as soon as reasonably possible. Records maintained in the database must be available for NRC review.

(7) If a licensee, applicant, or C/V administratively withdraws an individual's unescorted access authorization under the requirements of this section, the licensee, applicant, or C/V may not record the administrative action to withdraw the individual's unescorted access authorization as an unfavorable termination and may not disclose it in response to a suitable inquiry conducted under the provisions of part 26 of this chapter, a background investigation conducted under the provisions of this section, or any other inquiry or investigation. Immediately upon favorable completion of the background investigation element that caused the administrative withdrawal, the licensee, applicant, or C/V shall ensure that any matter that could link the individual to the temporary 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 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.

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.

(a)(1) The licensee shall assess and manage the potential for adverse affects on safety and security, including the site emergency plan, before implementing changes to plant configurations, facility conditions, or security.

(2) 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).

(b) 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.

15. In § 73.70, paragraph (c) is revised to read as follows:

§ 73.70 Records

* * * * *

(c) A register of visitors, vendors, and other individuals not employed by the licensee under §§ 73.46(d)(13), 73.55(g)(7)(ii), or 73.60. The licensee shall retain this register as a record, available for inspection, for three (3) years after the last entry is made in the register.

* * * * *

16. Section 73.71 is revised to read as follows:

§ 73.71 Reporting of safeguards events.

(a) Each licensee subject to the provisions of § 73.55 shall notify the NRC Operations Center,[1] as soon as possible but not later than 15 minutes after discovery of an imminent or actual safeguards threat against the facility and other safeguards events described in paragraph I of appendix G to this part.[2]

(1) When making a report under paragraph (a) of this section, the licensee shall:

(i) Identify the facility name; and

(ii) Briefly describe the nature of the threat or event, including:

(A) Type of threat or event (e.g., armed assault, vehicle bomb, credible bomb threat, etc.); and

(B) Threat or event status (i.e., imminent, in progress, or neutralized).

(2) Notifications must be made according to paragraph (e) of this section, as applicable.

(b) Each licensee subject to the provisions of §§ 73.25, 73.26, 73.27(c), 73.37, 73.67(e), or 73.67(g) shall notify the NRC Operations Center within one hour after discovery of the loss of any shipment of special nuclear material (SNM) or spent nuclear fuel, and within one hour after recovery of or accounting for the lost shipment. Notifications must be made according to paragraph (e) of this section, as applicable.

---

[1]Commercial (secure and non-secure) telephone numbers of the NRC Operations Center are specified in appendix A of this part.

[2] Notifications to the NRC for the declaration of an emergency class shall be performed in accordance with § 50.72 of this chapter.

(c) Each licensee subject to the provisions of §§ 73.20, 73.37, 73.50, 73.51, 73.55, 73.60, or 73.67 shall notify the NRC Operations Center within one hour after discovery of the safeguards events described in paragraph II of appendix G to this part. Notifications must be made according to paragraph (e) of this section, as applicable.

(d) Each licensee subject to the provisions of § 73.55 shall notify the NRC Operations Center, as soon as possible but not later than four (4) hours after discovery of the safeguards events described in paragraph III of appendix G to this part. Notifications must be made according to paragraph (e) of this section, as applicable.

(e) The licensee shall make the telephonic notifications required by paragraphs (a), (b), (c) and (d) of this section to the NRC Operations Center via the Emergency Notification System, or other dedicated telephonic system that may be designated by the Commission, if the licensee has access to that system.

(1) If the Emergency Notification System or other designated telephonic system is inoperative or unavailable, licensees shall make the required notification via commercial telephonic service or any other methods that will ensure that a report is received by the NRC Operations Center within the timeliness requirements of paragraphs (a), (b), (c), and (d) of this section, as applicable.

(2) The exception of § 73.21(g)(3) for emergency or extraordinary conditions applies to all telephonic reports required by this section.

(3) For events reported under paragraph (a) of this section, the licensee may be requested by the NRC to maintain an open, continuous communication channel with the NRC Operations Center, once the licensee has completed other required notifications under this section, § 50.72 of this chapter, or appendix E of part 50 of this chapter and any immediate actions to stabilize the plant. When established, the continuous communications channel shall be staffed by a knowledgeable individual in the licensee's security or operations organizations

(e.g., a security supervisor, an alarm station operator, operations personnel, etc.) from a location deemed appropriate by the licensee. The continuous communications channel may be established via the Emergency Notification System or dedicated telephonic system that may be designated by the Commission, if the licensee has access to these systems, or a commercial telephonic system.

(4) For events reported under paragraphs (b) or (c) of this section, the licensee shall maintain an open, continuous communication channel with the NRC Operations Center upon request from the NRC.

(5) For events reported under paragraph (d) of this section, the licensee is not required to maintain an open, continuous communication channel with the NRC Operations Center.

(f) Each licensee subject to the provisions of §§ 73.20, 73.37, 73.50, 73.51, 73.55, 73.60, or each licensee possessing SSNM and subject to the provisions of § 73.67(d) shall maintain a current safeguards event log.

(1) The licensee shall record the safeguards events described in paragraph IV of appendix G of this part within 24 hours of discovery.

(2) The licensee shall retain the log of events recorded under this section as a record for three (3) years after the last entry is made in each log or until termination of the license.

(g) Written reports.

(1) Each licensee making an initial telephonic notification under paragraphs (a), (b), and (c) of this section shall also submit a written report to the NRC within a 60 day period by an appropriate method listed in § 73.4.

(2) Licenses are not required to submit a written report following a telephonic notification made under paragraph (d) of this section.

(3) Each licensee shall submit to the Commission written reports that are of a quality that will permit legible reproduction and processing.

(4) Licensees subject to § 50.73 of this chapter shall prepare the written report on NRC Form 366.

(5) Licensees not subject to § 50.73 of this chapter shall prepare the written report in letter format.

(6) In addition to the addressees specified in § 73.4, the licensee shall also provide one copy of the written report addressed to the Director, Office of Nuclear Security and Incident Response.

(7) The report must include sufficient information for NRC analysis and evaluation.

(8) Significant supplemental information which becomes available after the initial telephonic notification to the NRC Operations Center or after the submission of the written report must be telephonically reported to the NRC Operations Center under paragraph (e) of this section and also submitted in a revised written report (with the revisions indicated) as required under paragraph (g)(6) of this section.

(9) Errors discovered in a written report must be corrected in a revised report with revisions indicated.

(10) The revised report must replace the previous report; the update must be complete and not be limited to only supplementary or revised information..

(11) Each licensee shall maintain a copy of the written report of an event submitted under this section as a record for a period of three (3) years from the date of the report.

(h) Duplicate reports are not required for events that are also reportable in accordance with §§ 50.72 and 50.73 of this chapter.

17. In appendix B to part 73, a new section VI is added to the table of contents, the introduction text is revised by adding a new paragraph between the first and second undesignated paragraphs, 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.

A. General requirements and introduction.

B. Employment suitability and qualification.

C. Duty training.

D. Duty qualification and requalification.

E. Weapons training.

F. Weapons qualification and requalification program.

G. Weapons, personnel equipment, and maintenance.

H. Records.

I. Audits and reviews.

J. Definitions.

Introduction

* * * * *

Applicants and power reactor licensees subject to the requirements of § 73.55 shall comply only with the requirements in 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.

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 members of the security organization, will be selected, trained, equipped, tested, and qualified.

4. Each individual assigned to perform security program duties and responsibilities required to effectively implement the Commission-approved security plans, licensee protective 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) An unarmed individual assigned to the security organization may not have any felony convictions that reflect on the individual's reliability.

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

2. Physical qualifications.

a. General physical qualifications.

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

(2) Armed and unarmed members of the security organization shall be subject to a physical examination designed to measure the individual's physical ability to perform assigned 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 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 members of the security organization 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 job 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 job duties during normal or emergency operations.

d. Existing medical conditions.

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

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

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

f. Other physical requirements. An individual who has been incapacitated due to a serious illness, injury, disease, or operation, which could interfere with the effective performance of assigned duties and responsibilities shall, before resumption of assigned duties and responsibilities, provide medical evidence of recovery and ability to perform these duties and responsibilities.

3. Psychological qualifications.

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

b. A licensed clinical 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 members of the security organization in addition to meeting the requirement stated in paragraph a. of this section, have no emotional instability that would interfere with the effective performance of assigned duties and responsibilities.

4. Medical examinations and physical fitness qualifications.

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. 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 job 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 members of the security organization 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 member of the security organization 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., before assignment, individuals 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 duties and responsibilities in accordance with the approved 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.

3. Tactical response team drills and exercises.

a. Licensees shall demonstrate response capabilities through a performance evaluation program as described in appendix C to this part.

b. The licensee shall conduct drills and exercises in accordance with Commission-approved security plans, licensee protective strategy, and implementing procedures.

(1) Drills and exercises must be designed to challenge participants in a manner which requires each participant to demonstrate requisite knowledge, skills, and abilities.

(2) Tabletop exercises may be used to supplement drills and exercises to accomplish desired training goals and objectives.

D. Duty qualification and requalification.

1. Qualification demonstration

a. Armed and unarmed members of the security organization 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 an annual written exam and hands-on performance demonstration.

(1) Written Exam. 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 Demonstration. Armed and unarmed members of the security organization 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.

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 members of the security organization 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, qualification scores, 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 re-certification 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, range penetration capability of weapon, and bull's-eye firing.

(2) Weapons cleaning and storage.

(3) Combat firing, day and night.

(4) Safe weapons handling.

(5) Clearing, loading, unloading, and reloading.

(6) When to draw and point a weapon.

(7) Rapid fire techniques.

(8) Closed quarter firing.

(9) Stress firing.

(10) Zeroing assigned weapon(s) (sight and sight/scope adjustments).

(11) Target engagement.

(12) Weapon malfunctions.

(13) Cover and concealment.

(14) Weapon transition between strong (primary) and weak (support) hands.

(15) 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.

c. Each individual shall be re-qualified at least annually.

2. Alternate weapons qualification. Upon written request by the licensee, the Commission may authorize an applicant or licensee to provide firearms qualification programs other than those listed in this appendix if the applicant or licensee demonstrates that the alternative firearm qualification program satisfies Commission requirements. Written requests must provide regarding the proposed firearms qualification programs and describe how the proposed alternative satisfies Commission requirements.

3. 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 qualification and re-qualification courses for each firearm 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.

4. Firearms qualification courses. The licensee shall conduct the following qualification courses for weapons 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.

5. Courses of fire.

a. Handgun.

(1) 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 and scores established by a law enforcement course, or an equivalent nationally recognized course.

(2) Qualifying scores must be an accumulated total of 70 percent of the maximum obtainable target score.

b. Semiautomatic rifle.

(1) Armed members of the security organization, assigned duties and responsibilities involving the use of a semiautomatic rifle shall qualify in accordance with the standards and scores established by a law enforcement course, or an equivalent nationally recognized course.

(2) Qualifying scores must be an accumulated total of 80 percent of the maximum obtainable score.

c. Shotgun.

(1) Armed members of the security organization, assigned duties and responsibilities involving the use of a shotgun shall qualify in accordance with standards and scores established by a law enforcement course, or an equivalent nationally recognized course.

(2) Qualifying scores must be an accumulated total of 70 percent of the maximum obtainable target score.

d. Enhanced weapons.

(1) Armed members of the security organization, assigned duties and responsibilities involving the use of any weapon or weapons not described above, shall qualify in accordance with applicable standards and scores established by a law enforcement course or an equivalent nationally recognized course for these weapons.

(2) Qualifying scores must be an accumulated total of 80 percent of the maximum obtainable score.

6. 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.

b. Firearms requalification must be conducted using the courses of fire outlined in Paragraph 5 of this section

G. Weapons, personal equipment, and maintenance.

1. Weapons.

a. 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, 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) Duress alarms.

(5) Two-way portable radios (handi-talkie) 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, 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) Tear gas or other non-lethal gas.

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 superceded.

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

I. Audits and reviews.

The licensee shall review the Commission-approved training and qualification plan 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.

18. In appendix C to part 73, a heading for Section I and a new introductory paragraph are added after the “Introduction” section and before the heading “Contents of the Plan,” and a new Section II is added at the end of the appendix to read as follows:

APPENDIX C TO PART 73—LICENSEE SAFEGUARDS CONTINGENCY PLANS

* * * * *

Section I: Safeguards contingency plans.

Introduction

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 of this appendix.

* * * * *

Section II: Nuclear power plant safeguards contingency plans.

(a) Introduction

The safeguards contingency plan must describe how the criteria set forth in this appendix will be satisfied through implementation and must provide specific goals, objectives and general guidance to licensee personnel to facilitate the initiation and completion of predetermined and exercised responses to threats, up to and including the design basis threat described in § 73.1(a)(1).

Contents of the plan.

(b) Each safeguards contingency plan must include the following twelve (12) categories of information:

(1) Background.

(2) Generic Planning Base.

(3) Licensee Planning Base.

(4) Responsibility Matrix.

(5) Primary Security Functions.

(6) Response Capabilities.

(7) Protective Strategy.

(8) Integrated Response Plan.

(9) Threat Warning System.

(10) Performance Evaluation Program.

(11) Audits and Reviews.

(12) Implementing Procedures.

(c) Background.

(1) 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.

(2) Licensees shall describe the general goals and operational concepts underlying implementation of the approved safeguards contingency plan, to include, but not limited to the following:

(i) The types of incidents covered.

(ii) The specific goals and objectives to be accomplished.

(iii) The different elements of the onsite physical protection program that are used to provide at all times the capability to detect, assess, intercept, challenge, delay, and neutralize

threats up to and including the design basis threat relative to the perceived dangers and incidents described in the Commission-approved safeguards contingency plan.

(iv) How the onsite response effort is organized and coordinated to ensure that licensees capability to prevent significant core damage and spent fuel sabotage is maintained throughout each type of incident covered.

(v) How the onsite response effort is integrated to include specific procedures, guidance, and strategies to maintain or restore core cooling, containment, and spent fuel pool cooling capabilities using existing or readily available resources (equipment and personnel) that can be effectively implemented under the circumstances associated with loss of large areas of the plant due to explosions or fires.

(vi) A list of terms and their definitions used in describing operational and technical aspects of the approved safeguards contingency plan.

(d) Generic planning base.

(1) Licensees shall define the criteria for initiation and termination of responses to threats to include the specific decisions, actions, and supporting information needed to respond to each type of incident covered by the approved safeguards contingency plan.

(2) Licensees shall ensure early detection of unauthorized activities and shall respond to all alarms or other indications of a threat condition such as, tampering, bomb threats, unauthorized barrier penetration (vehicle or personnel), missing or unaccounted for nuclear material, escalating civil disturbances, imminent threat notification, or other threat warnings.

(3) The safeguards contingency plan must:

(i) Identify the types of events that signal the beginning or initiation of a safeguards contingency event.

(ii) Provide predetermined and structured responses to each type of postulated event.

(iii) Define specific goals and objectives for response to each postulated event.

(iv) Identify the predetermined decisions and actions which are required to satisfy the written goals and objectives for each postulated event.

(v) Identify the data, criteria, procedures, mechanisms and logistical support necessary to implement the predetermined decisions and actions.

(vi) Identify the individuals, groups, or organizational entities responsible for each predetermined decision and action.

(vii) Define the command-and-control structure required to coordinate each individual, group, or organizational entity carrying out predetermined actions.

(viii) Describe how effectiveness will be measured and demonstrated to include the effectiveness of the capability to detect, assess, intercept, challenge, delay, and neutralize threats up to and including the design basis threat.

(e) Licensee planning base.

Licensees shall describe the site-specific factors affecting contingency planning and shall develop plans for actions to be taken in response to postulated threats. The following topics must be addressed:

(1) Organizational Structure. The safeguards contingency plan must describe the organization's chain of command and delegation of authority during safeguards contingencies, to include a description of how command-and-control functions will be coordinated and maintained.

(2) Physical layout.

(i) The safeguards contingency plan must include a site description, to include maps and drawings, of the physical structures and their locations.

(A) Site Description. The site description must address the site location in relation to nearby towns, transportation routes (e.g., rail, water, air, roads), pipelines, hazardous material

facilities, onsite independent spent fuel storage installations, and pertinent environmental features that may have an effect upon coordination of response operations.

(B) Approaches. Particular emphasis must be placed on main and alternate entry routes for law-enforcement or other offsite support agencies and the location of control points for marshaling and coordinating response activities.

(ii) Licensees with co-located Independent Spent Fuel Storage Installations shall describe response procedures for both the operating reactor and the Independent Spent Fuel Storage Installation to include how onsite and offsite responders will be coordinated and used for incidents occurring outside the protected area.

(3) Safeguards Systems Hardware. The safeguards contingency plan must contain a description of the physical security and material accounting system hardware that influence how the licensee will respond to an event.

(4) Law enforcement assistance.

(i) The safeguards contingency plan must contain a listing of available local, state, and Federal law enforcement agencies and a general description of response capabilities, to include number of personnel, types of weapons, and estimated response time lines.

(ii) The safeguards contingency plan must contain a discussion of working agreements with offsite law enforcement agencies to include criteria for response, command and control protocols, and communication procedures.

(5) Policy constraints and assumptions. The safeguards contingency plan must 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.

(6) Administrative and logistical considerations. The safeguards contingency plan must contain a description of licensee practices which influence how the licensee responds to a threat to include, but not limited to, a description of the procedures that will be used for ensuring that all equipment needed to effect a successful response will be readily accessible, in good working order, and in sufficient supply to provide redundancy in case of equipment failure.

(f) Responsibility matrix.

(1) The safeguards contingency plan must describe the organizational entities that are responsible for each decision and action associated with responses to threats.

(i) For each identified initiating event, a tabulation must be made for each response depicting the assignment of responsibilities for all decisions and actions to be taken.

(ii) The tabulations described in the responsibility matrix must provide an overall description of response actions and interrelationships.

(2) Licensees shall ensure that duties and responsibilities required by the approved safeguards contingency plan do not conflict with or prevent the execution of other site emergency plans.

(3) Licensees shall identify and discuss potential areas of conflict between site plans in the integrated response plan required by Section II(b)(8) of this appendix.

(4) Licensees shall address safety/security interface issues in accordance with the requirements of § 73.58 to ensure activities by the security organization, maintenance, operations, and other onsite entities are coordinated in a manner that precludes conflict during both normal and emergency conditions.

(g) Primary security functions.

(1) Licensees shall establish and maintain at all times, the capability to detect, assess, and respond to all threats to the facility up to and including the design basis threat.

(2) To facilitate initial response to a threat, licensees shall ensure the capability to observe all areas of the facility in a manner that ensures early detection of unauthorized activities and limits exposure of responding personnel to possible attack.

(3) Licensees shall generally describe how the primary security functions are integrated to provide defense-in-depth and are maintained despite the loss of any single element of the onsite physical protection program.

(4) Licensees description must begin with physical protection measures implemented in the outermost facility perimeter, and must move inward through those measures implemented to protect vital and target set equipment.

(h) Response capabilities.

(1) Licensees shall establish and maintain at all times the capability to intercept, challenge, delay, and neutralize threats up to and including the design basis threat.

(2) Licensees shall identify the personnel, equipment, and resources necessary to perform the actions required to prevent significant core damage and spent fuel sabotage in response to postulated events.

(3) Licensees shall ensure that predetermined actions can be completed under the postulated conditions.

(4) Licensees shall provide at all times an armed response team comprised of trained and qualified personnel who possess the knowledge, skills, abilities, and equipment required to implement the Commission-approved safeguards contingency plan and site protective strategy. The plan must include a description of the armed response team including the following:

(i) The authorized minimum number of armed responders, available at all times inside the protected area.

(ii) The authorized minimum number of armed security officers, available onsite at all times.

(5) The total number of armed responders and armed security officers must be documented in the approved security plans and documented as a component of the protective strategy.

(6) Licensees shall ensure that individuals assigned duties and responsibilities to implement the Safeguards Contingency Plan are trained and qualified in accordance with appendix B of this part and the Commission-approved security plans.

(i) Protective strategy.

(1) Licensees shall develop, maintain, and implement a written protective strategy that describes the deployment of the armed response team relative to the general goals, operational concepts, performance objectives, and specific actions to be accomplished by each individual in response to postulated events.

(2) The protective strategy must:

(i) Be designed to prevent significant core damage and spent fuel sabotage through the coordinated implementation of specific actions and strategies required to intercept, challenge, delay, and neutralize threats up to and including the design basis threat of radiological sabotage.

(ii) Describe and consider site specific conditions, to include but not limited to, facility layout, the location of target set equipment and elements, target set equipment that is in maintenance or out of service, and the potential effects that unauthorized electronic access to safety and security systems may have on the protective strategy capability to prevent significant core damage and spent fuel sabotage.

(iii) Identify predetermined actions and time lines for the deployment of armed personnel.

(iv) Provide bullet resisting protected positions with appropriate fields of fire.

(v) Limit exposure of security personnel to possible attack.

(3) Licensees shall 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 and that facilitates response in accordance with the integrated response plan.

(j) Integrated Response Plan

(1) Licensees shall document, maintain, and implement an Integrated Response Plan which must identify, describe, and coordinate actions to be taken by licensee personnel and offsite agencies during a contingency event or other emergency situation.

(2) The Integrated Response Plan must:

(i) Be designed to integrate and coordinate all actions to be taken in response to an emergency event in a manner that will ensure that each site plan and procedure can be successfully implemented without conflict from other plans and procedures.

(ii) Include specific procedures, guidance, and strategies to maintain or restore core cooling, containment, and spent fuel pool cooling capabilities using existing or readily available resources (equipment and personnel) that can be effectively implemented under the circumstances associated with loss of large areas of the plant due to explosions or fires.

(iii) Ensure that onsite staffing levels, facilities, and equipment required for response to any identified event, are readily available and capable of fulfilling their intended purpose.

(iv) Provide emergency action levels to ensure that threats result in at least a notification of unusual event and implement procedures for the assignment of a predetermined classification to specific events.

(v) Include specific procedures, guidance, and strategies describing cyber incident response and recovery.

(3) Licensees shall:

(i) Reconfirm on a annual basis, liaison with local, state, and Federal law enforcement agencies, established in accordance with § 73.55(k)(8), to include communication protocols,

command and control structure, marshaling locations, estimated response times, and anticipated response capabilities and specialized equipment.

(ii) Provide required training to include simulator training for the operations response to security events (e.g. loss of ultimate heat sink) for nuclear power reactor personnel in accordance with site procedures to ensure the operational readiness of personnel commensurate with assigned duties and responsibilities.

(iii) Periodically train personnel in accordance with site procedures to respond to a hostage or duress situation.

(iv) Determine the possible effects that nearby hazardous material facilities may have upon site response plans and modify response plans, procedures, and equipment as necessary.

(v) Ensure that identified actions are achievable under postulated conditions.

(k) Threat warning system.

(1) Licensees shall implement a “Threat warning system” which identifies specific graduated protective measures and actions to be taken to increase licensee preparedness against a heightened or imminent threat of attack.

(2) Licensees shall ensure that the specific protective measures and actions identified for each threat level are consistent with the Commission-approved safeguards contingency plan, and other site security, and emergency plans and procedures.

(3) Upon notification by an authorized representative of the Commission, licensees shall implement the specific protective measures assigned to the threat level indicated by the Commission representative.

(l) Performance Evaluation Program

(1) Licensees shall document and maintain a Performance Evaluation Program that describes how the licensee will demonstrate and assess the effectiveness of the onsite physical

protection program to prevent significant core damage and spent fuel sabotage, and to include the capability of armed personnel to carry out their assigned duties and responsibilities.

(2) The Performance Evaluation Program must include procedures for the conduct of quarterly drills and annual force-on-force exercises that are designed to demonstrate the effectiveness of the licensee's capability to detect, assess, intercept, challenge, delay, and neutralize a simulated threat.

(i) The scope of drills conducted for training purposes must be determined by the licensee as needed, and can be limited to specific portions of the site protective strategy.

(ii) Drills, exercises, and other training must be conducted under conditions that simulate as closely as practical the site specific conditions under which each member will, or may be, required to perform assigned duties and responsibilities.

(iii) Licensees shall document each performance evaluation to include, but not limited to, scenarios, participants, and critiques.

(iv) Each drill and exercise must include a documented post exercise critique in which participants identify failures, deficiencies, or other findings in performance, plans, equipment, or strategies.

(v) Licensees shall enter all findings, deficiencies, and failures identified by each performance evaluation into the corrective action program to ensure that timely corrections are made to the onsite physical protection program and necessary changes are made to the approved security plans, licensee protective strategy, and implementing procedures.

(vi) Licensees shall protect all findings, deficiencies, and failures relative to the effectiveness of the onsite physical protection program in accordance with the requirements of § 73.21.

(3) For the purpose of drills and exercises, licensees shall:

(i) Use no more than the number of armed personnel specified in the approved security plans to demonstrate effectiveness.

(ii) Minimize the number and effects of artificialities associated with drills and exercises.

(iii) Implement the use of systems or methodologies that simulate the realities of armed engagement through visual and audible means, and reflects the capabilities of armed personnel to neutralize a target though the use of firearms during drills and exercises.

(iv) Ensure that each scenario used is capable of challenging the ability of armed personnel to perform assigned duties and implement required elements of the protective strategy.

(4) The Performance Evaluation Program must be designed to ensure that:

(i) Each member of each shift who is assigned duties and responsibilities required to implement the approved safeguards contingency plan and licensee protective strategy participates in at least one (1) drill on a quarterly basis and one (1) force on force exercise on an annual basis.

(ii) The mock adversary force replicates, as closely as possible, adversary characteristics and capabilities in the design basis threat described in § 73.1(a)(1), and is capable of exploiting and challenging the licensee protective strategy, personnel, command and control, and implementing procedures.

(iii) Protective strategies are evaluated and challenged through tabletop demonstrations.

(iv) Drill and exercise controllers are trained and qualified to ensure each controller has the requisite knowledge and experience to control and evaluate exercises.

(v) Drills and exercises are conducted safely in accordance with site safety plans.

(5) 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.

(6) Scenarios.

(i) Licensees shall develop and document multiple scenarios for use in conducting quarterly drills and annual force-on-force exercises.

(ii) Licensee scenarios must be designed to test and challenge any component or combination of components, of the onsite physical protection program and protective strategy.

(iii) 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.

(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.

(m) Records, audits, and reviews.

(1) Licensees shall review and audit the Commission-approved safeguards contingency plan in accordance with the requirements § 73.55(n) of this part.

(2) The licensee shall make necessary adjustments to the Commission-approved safeguards contingency plan to ensure successful implementation of Commission regulations and the site protective strategy.

(3) The safeguards contingency plan review must include an audit of implementing procedures and practices, the site protective strategy, and response agreements made by local, state, and Federal law enforcement authorities.

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

(n) Implementing procedures.

(1) 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 Commission- approved security plans and the site protective strategy.

(2) Licensees shall ensure that implementing procedures accurately reflect the information contained in the Responsibility Matrix required by this appendix, the Commission-approved security plans, the Integrated Response Plan, and other site plans.

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

19. 10 CFR part 73, appendix G, is revised to read as follows:

APPENDIX G TO PART 73—REPORTABLE SAFEGUARDS EVENTS

Under the provisions of § 73.71(a), (d), and (f) of this part, licensees subject to the provisions of § 73.55 of this part shall report or record, as appropriate, the following safeguards events under paragraphs I, II, III, and IV of this appendix. Under the provisions of § 73.71(b), (c), and (f) of this part, licensees subject to the provisions of §§ 73.20, 73.37, 73.50, 73.60, and 73.67 of this part shall report or record, as appropriate, the following safeguards events under paragraphs II and IV of this appendix. Licensees shall make such reports to the Commission under the provisions of § 73.71 of this part.

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

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

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

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

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

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

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

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

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

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

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

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

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

(1) Any security-related incident involving suspicious activity that may be indicative of potential pre-operational surveillance, reconnaissance, or intelligence-gathering activities directed against the facility. Such activity may include, but is not limited to, attempted surveillance or reconnaissance activity, elicitation of information from security or other site personnel relating to the security or safe operation of the plant, or challenges to security systems (e.g., failure to stop for security checkpoints, possible tests of security response and security screening equipment, or suspicious entry of watercraft into posted off-limits areas).

(2) Any security-related incident involving suspicious aircraft overflight activity. Commercial or military aircraft activity considered routine by the licensee is not required to be reported.

(3) Incidents resulting in the notification of local, state or national law enforcement, or law enforcement response to the site not included in paragraphs I or II of this appendix;

(b) The unauthorized use of or tampering with the components or controls, including the security system, of nuclear power reactors.

(c) Follow-up communications regarding events reported under paragraph III of this appendix will be completed through the NRC threat assessment process via the NRC Operations Center.[1]

IV. Events to be recorded within 24 hours of discovery in the safeguards event log.

(a) Any failure, degradation, or discovered vulnerability in a safeguards system that could have allowed unauthorized or undetected access to any area or transport in which the

[1]Commercial (secure and non-secure) telephone numbers of the NRC Operations Center are specified in appendix A of this part.

licensee is required by Commission regulations to control access had compensatory measures not been established.

(b) Any other threatened, attempted, or committed act not previously defined in this appendix with the potential for reducing the effectiveness of the physical protection program below that described in a licensee physical security or safeguards contingency plan, or the actual condition of such reduction in effectiveness.

Dated at Rockville, Maryland, this 10th day of October 2006.

For the Nuclear Regulatory Commission.

/ s /

Annette L. Vietti-Cook,
Secretary of the Commission.