[7590-01-P]

NUCLEAR REGULATORY COMMISSION

10 CFR Parts 60, 63, 73, and 74

RIN: 3150-AI06

Geologic Repository Operations Area Security and
Material Control and Accounting Requirements

AGENCY: Nuclear Regulatory Commission.

ACTION: Proposed rule.

SUMMARY: The Nuclear Regulatory Commission (NRC) is proposing to amend its regulations to revise the security requirements and material control and accounting (MC&A) requirements for a geologic repository operations area (GROA). The goal of this rulemaking is to ensure that effective security measures are in place for the protection of high-level radioactive waste (HLW) and other radioactive material at a GROA given the post-September 11, 2001, threat environment. New requirements for specific training enhancements, improved access authorization, enhancements to defensive strategies, and enhanced reporting requirements would be incorporated. The proposed rule would establish general performance objectives and corresponding system capabilities for the GROA MC&A program, with a focus on strengthening, streamlining, and consolidating all MC&A regulations specific to a GROA. In addition, the proposed rule would require the emergency plan to address radiological emergencies.

DATES: The comment period expires (**insert 75 days from date of publication in the**

Federal Register). Comments received after this date will be considered if it is practical to do so, but the NRC is able to assure consideration only for comments received on or before this date.

ADDRESSES: You may submit comments by any one of the following methods. Please include the number RIN 3150-AI06 in the subject line of your comments. Comments on rulemakings submitted in writing or in electronic form will be made available to the public in their entirety on the NRC rulemaking website. Personal information such as name, address, telephone, e-mail address, etc., will not be removed from your submission.

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 website to Carol Gallagher (301) 415-5905; email cag@nrc.gov.

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

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

Publicly available documents related to this rulemaking may be examined and copied for a fee at the NRC's Public Document Room (PDR), Public File Area O1 F21, One White Flint North, 11555 Rockville Pike, Rockville, Maryland 20852. Selected documents, including comments, can be viewed and downloaded electronically via the NRC rulemaking website 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/NRC/ADAMS/index.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: Merri Horn, Office of Federal and State Materials and Environmental Management Programs, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, telephone (301) 415-8126, e-mail, mlh1@nrc.gov.

SUPPLEMENTARY INFORMATION:

H. Would Shipper-Receiver Comparisons with Independent Measurements be Required for Receipts?

I. What Measurements Would be Necessary Under the GROA MC&A Program?

J. What Would an MC&A Detection and Response Program Involve?

K. What Additional Requirements Would be Imposed if DOE Possesses Formula Quantities of Strategic SNM that is in a Form Other than as Irradiated Nuclear Reactor Fuel?

L. What Special MC&A-Related Needs Exist?

M. What is the Objective of the Proposed Physical Security Requirements?

N. What Threat Would a GROA be Required to Defend Against?

O. Why do the Security Requirements Differ for Various Aspects of a GROA?

P. Would Access Authorization Requirements Apply to a GROA and What Would They Cover?

Q. Would Criminal History Checks Apply to a GROA?

R. What are the Key Aspects of the Security Requirements?

S. What is a Target Set as it Applies to a GROA?

T. What Weapons Authorization Would be Necessary for the GROA Operations?

U. Would DOE be Required to Conduct Force-on-Force Exercises for the GROA Facility?

V. How Would the Security Plans Handle Construction at a GROA After Receipt of HLW Begins?

W. Does this Rulemaking Cover Transportation of High-Level Radioactive Waste to a GROA?

X. Would the Security and MC&A Plans Cover Postclosure?

Y. What Safeguards Reporting Requirements Would be Proposed for a GROA?

Z. Does the NRC Plan to Issue Guidance Documents?

AA. Would the GROA Facilities be Subject to IAEA Safeguards?

BB. What Changes Would be Made to the Emergency Plan Requirements?

I. Background

On November 2, 2001 (66 FR 55732), the NRC published its final rule governing disposal of HLW in a potential geologic repository at Yucca Mountain in Nevada. The U.S. Department of Energy (DOE) must comply with these regulations for NRC to authorize construction and license operation of a potential repository at Yucca Mountain in Nevada. The security requirements applicable to a GROA in these regulations were developed prior to September 11, 2001, under a previous and very different threat environment. Currently, there is no distinction between the security and MC&A requirements for independent spent fuel storage installations (ISFSIs) and the requirements for larger, more complicated geologic repositories for permanent disposal of HLW. At the time the security provisions were

established, the NRC used the same regulatory approach for protecting a GROA as that for protecting spent nuclear fuel storage facilities licensed under 10 CFR Part 72. GROA operations, at least those conducted in surface facilities, seemed vulnerable to the same kinds of potential threats that were characteristic of the storage of spent nuclear fuel (SNF). The same level of protection was deemed sufficient to protect against acts that might be inimical to the common defense and security. The same reasoning applies to the MC&A requirements.

The NRC's regulatory approach was predicated on maintaining the physical integrity of the SNF rods. In the event the physical integrity of the SNF rods could not be maintained, the staff planned to address the additional security measures that would be necessary by incorporating conditions into the license.

Potential surface operations at a GROA have become more complex over the years. For example, the DOE has indicated that it now plans to include bare SNF handling operations within a spent fuel pool to transfer SNF from a non-TAD (transfer, aging, disposal) canister to a TAD canister, which would then be utilized for emplacement and permanent disposal of the SNF in the Yucca Mountain repository.

Because both the threat environment and the plans for surface operations at the GROA have changed, the NRC now believes that a separate regulatory approach for protecting and safeguarding a GROA is necessary. The DOE has not set forth a final concept of operations for the GROA. Therefore, it is not clear what types of facilities will be part of the surface operations or what type of handling of the HLW within the surface facilities may occur.

The new security and MC&A requirements also should be broad enough and sufficiently flexible to cover a range of possible types of non-HLW radioactive materials without the need for additional rulemaking. The DOE, in its Final Environmental Impact Statement (FEIS) for a geologic repository at Yucca Mountain, considered the possibility that radioactive waste types

other than SNF and HLW, such as Greater-Than-Class-C low-level radioactive waste (LLW) and Special-Performance-Assessment-Required LLW might be disposed of in a geologic repository. See Final Environmental Impact Statement for a Geologic Repository for the Disposal of Spent Nuclear Fuel and High-Level Radioactive Waste at Yucca Mountain, Nye County, Nevada, February 2002, Vol. II, A-1, A-57 - A-64. Disposal of such non-HLW could require new legislation or a determination by the NRC that these wastes require permanent isolation. The NRC is not making such a determination in this rulemaking. However, the security and MC&A requirements being proposed for a GROA take account of the possibility that the geologic repository might be used for the disposal of radioactive materials which are not SNF or HLW.

Following the terrorist attacks on September 11, 2001, the NRC conducted a thorough review of its security requirements to ensure that special nuclear material (SNM) at fixed sites and in transit continued to have effective security measures in place given the changing threat environment. Through a series of security orders issued to certain NRC licensees, the Commission specified changes to the Design Basis Threat (DBT) for power reactor and Category I Strategic SNM licensees, and implemented enhanced requirements for specific training, access authorization, defensive strategies, and security. Through generic communications, the Commission specified expectations about enhanced notifications to the NRC for certain security events or suspicious activities. These enhancements resulted in some licensees revising their physical security plans, security personnel training and qualification plans, and safeguards contingency plans to defend against the supplemental DBT requirements. These security orders specifically required certain licensees to: (1) increase patrols; (2) augment the security force capabilities and security posts; (3) add and modify existing physical security barriers; (4) move vehicle check points to a greater standoff distance;

(5) enhance coordination with local law enforcement agency (LLEA) and military authorities; (6) augment their security and emergency response training, equipment, and communications; and (7) strengthen off-site access controls, including additional background and screening checks of employees. The enhanced security measures have yet to be imposed on a GROA. This rulemaking is the mechanism the NRC is using to impose the new requirements on the DOE for operations at a GROA.

This rulemaking to upgrade the requirements for physical protection of HLW and other radioactive materials at a GROA combines lessons learned, current/best practices, and requirements based on those contained in security orders issued to NRC licensees that address the post-September 11, 2001, threat environment. The security orders, as well as other ongoing security rulemakings, are used as the basis for upgrading the GROA security requirements. Specifically, the security requirements for power reactors are being used as the starting point for the security requirements for this proposed rule. The reactor requirements are used as the stating point because of the similarity in material, the material's attractiveness for malevolent use, and the potential consequences of its malevolent use. The security requirements should provide protection equivalent to a power reactor. The reactor requirements have been proposed in a rule entitled "Power Reactor Security Requirements" (71 FR 62664; October 26, 2006).

Section 653 of the Energy Policy Act of 2005 (EPAct), signed into law on August 8, 2005, 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 requires that all security personnel with access to any weapons undergo a background check that includes fingerprinting and a check against the Federal Bureau of Investigation's (FBI) National Instant Criminal Background Check System (NICS) database.

Under Section 161k. of the Atomic Energy Act (AEA), as amended, the DOE has authority for authorization of weapons. The NRC does not plan to use its authority under Section 653 of the EPAct. The DOE, under its own authority under Section 161k. of the AEA, may authorize the use of an expanded weapons arsenal and the use of force in accordance with the requirements of 10 CFR Part 1047.

The goal of this rulemaking is to ensure that effective security measures are in place for the protection of HLW and other radioactive materials given the post-September 11, 2001, threat environment. New requirements for specific training enhancements, improved access authorization, and enhancements to defensive strategies would be incorporated. The proposed rule would establish general performance objectives and corresponding system capabilities for the GROA MC&A program, with a focus on strengthening, streamlining, and consolidating into 10 CFR Part 74 all MC&A regulations specific to a GROA. In addition, the proposed rule would require the emergency plan to address radiological emergencies.

II. Discussion

A. *What Action is the NRC Taking?*

The NRC is proposing to amend its regulations primarily to establish new physical security and MC&A requirements for HLW and other radioactive materials at a GROA. The requirements specified in this rulemaking would establish the objectives and minimum performance standards that the DOE must meet to protect against each threat (theft or diversion and radiological sabotage) at a GROA, and the objectives and minimum capabilities for the MC&A program. The proposed rule is risk-informed and performance-based.

B. *Whom Would This Action Affect?*

Only the DOE, as the potential operator of any repository, would be impacted by this proposed rule. The regulations in 10 CFR Part 63 are specific for the Yucca Mountain repository.

C. *Why do the Requirements Need to be Revised?*

The current regulations for MC&A and security for a GROA were developed under a different threat environment, and the threat environment has changed, as have the plans for surface operations at a GROA. The NRC now believes that a new regulatory approach for protecting a GROA is necessary. In addition, the DOE has not set forth a final concept of operations document for the GROA; therefore, the types and forms of material to be handled and disposed of at a GROA have not been finalized. The current security and MC&A requirements for a GROA are not adequate to protect the common defense and security or the public health and safety. The new security and MC&A requirements must be broad enough and sufficiently flexible to cover a range of possible activities without the need for additional rulemaking. This rulemaking to upgrade the requirements for physical protection of HLW and other radioactive materials at a GROA capitalizes on the lessons learned, current/best practices, and security orders issued to NRC licensees to address the post-September 11, 2001, threat environment. The security orders, as well as ongoing security rulemakings, have been used as the basis for upgrading the GROA security requirements. The proposed rule would also establish general performance objectives and corresponding system capabilities for the GROA MC&A program, with a particular focus on strengthening, streamlining, and consolidating into 10 CFR Part 74 all MC&A regulations specific to a GROA.

D. *When do the Security and MC&A Plans Need to be Submitted?*

The DOE should include a description of the security and MC&A plans in its license application when it is submitted. The actual plans would be submitted no later than 180 days

after the Commission grants the construction authorization for the GROA. A description of the security and MC&A plans is necessary at the time of the application to demonstrate that the DOE can adequately address and meet the NRC requirements for security and MC&A. Additionally, there may be some aspects that would be better integrated during construction. Submitting the plans after the Commission grants a construction authorization allows the DOE to take advantage of any new technology and concepts that may not be available at the time the construction application is submitted. The timing still allows some aspects, if appropriate, to be addressed during construction. The plans would not need to be implemented until the Commission grants a license to receive and possess source, special nuclear, or byproduct material at a GROA.

E. *What Types of Material Would be Covered by the New Security and MC&A Requirements?*

This rule would cover the security and MC&A aspects for the radioactive material at both surface and subsurface areas where waste handling activities are conducted. This radioactive material can include HLW in the form of irradiated reactor fuel and reprocessing wastes. Section 63.102(b)(4) provides that if the DOE proposes to use the GROA for storage of radioactive waste other than HLW, the storage of this radioactive waste is subject to the requirements of 10 CFR Part 63. Irradiated reactor fuel contains SNM and fission byproducts. Depending on the enrichment and quantity, the SNM may be considered strategic special nuclear material, SNM of moderate strategic significance, or SNM of low strategic significance. The higher the enrichment of the SNM, the more attractive the material may be for malevolent purposes. While it is expected that the primary waste to be handled at a GROA is irradiated reactor fuel, it is possible that the DOE may propose the storage of other types of radioactive waste. Therefore, the Commission has attempted in this proposed rule to develop security and MC&A requirements that are broad enough to cover the spectrum of waste materials that could

potentially be dispositioned at a GROA without the need for future rulemaking. The security requirements that would be established are, in part, based on the attractiveness of the waste material, shape, size, and the potential consequences if the waste were used for malevolent purposes. The MC&A requirements pertain to the SNM content of the waste.

F. *What are the Key Aspects of the Proposed MC&A Requirements?*

The proposed rule would establish general performance objectives and corresponding systems capabilities for the GROA MC&A program, with a particular focus on strengthening, streamlining, and consolidating in 10 CFR Part 74 all MC&A regulations specific to a GROA. Proposed objectives for the GROA MC&A program would center on detecting and responding to a potential loss of SNM, including theft and diversion, commensurate with the strategic worth of the SNM. The DOE would be required to submit an MC&A plan describing how those objectives would be achieved through the implementation of specified system capabilities commensurate with safeguards risks.

G. *What Kinds of Systems Capabilities Would be Proposed for the MC&A Program?*

The DOE would be required to establish and maintain internal control, inventory, auditing, and recordkeeping capabilities. Internal controls would include comprehensive measures for management structuring, personnel qualification and training, validating receipts and any shipments, item control, collusion protection, measurements, and measurement control for resolving anomalies (as needed). This would include an overall detection and response program and a collusion program to thwart theft or diversion and would include incorporating checks and balances that are sufficient to detect falsification of data and reports that could conceal the theft or diversion of SNM.

Item control of SNM and continuous assurance of its integrity from receipt to emplacement would be important. If necessary, additional item control and physical inventory

measures may be required for recovery of waste packages or retrieval of waste packages from emplacement in Yucca Mountain to an alternate storage or an area for possible examination or external shipment.

H. *Would Shipper-Receiver Comparisons with Independent Measurements be Required for Receipts?*

No, the DOE would not be required to conduct independent measurements on receipts of HLW or SNM at a GROA. The DOE would be allowed to accept the originator-assigned values. However, the DOE would be required to routinely assure the validity of each originator's assigned SNM content values and the integrity of receipts (with validating physical checking of unique identity, intactness, and tamper-safing) accepted at a GROA. No routine nondestructive assay (NDA) measurements of receipts would be required. The DOE would be required to closely coordinate with originators to adequately understand the technical basis for assigning SNM content and procedures to be followed for packaging and assuring item identification and integrity, (e.g., with reactor fuel burnup calculations, unique serial numbers, and the tamper-safing of canisters and shipment overpacts). Tamper-safing refers to the use of devices on containers in a manner that ensures a clear indication if the device has been removed to allow opening of the container.

For shipments of commercial SNF to the proposed Yucca Mountain repository, the DOE is currently expected to be the shipper as the DOE is expected to take possession of the material at the nuclear reactor. However, for the purposes of reporting to the Nuclear Material Management Safeguards System (NMMSS), power reactor utilities would be expected to complete and file the The DOE/NRC Form-741 for transferring the SNM to the GROA using their respective NRC Reporting Identification Symbol (RIS). As a result, following the instructions in NUREG/BR-0007 and NMMSS Report D-24, the transfer for MC&A technical

purposes would be made between two NRC RISs - from a power reactor utility RIS to that assigned to the GROA for receiving and possessing SNM under license. This is not a new requirement as licensees are currently required to report transfers of SNM. In their reference to shippers, the MC&A regulations at § 74.15 are addressing the licensed utilities who are originating and reporting the transfers with SNM content values technically assigned by the utility. Any required tamper-safing of shipments to assure their integrity (e.g., the welding of canisters or the affixing of tamper-indicating devices on shipping overpacts) would also be done by such originating shippers from a shipper-receiver validation/comparison.

I. *What Measurements Would be Necessary Under the GROA MC&A Program?*

As warranted, independent confirmatory weight and NDA measurements of HLW and SNM would be required for off-normal circumstances (e.g., in resolving certain types of anomalies that may arise and trigger investigations and special reporting of safeguards events). The state-of-the-art for NDA and other practical limitations shall be considered for such nonroutine measurements (e.g., at a wet transfer facility where bare spent fuel assemblies may be handled). At this point, no routine onsite measurements are foreseen as necessary to further validate/accept SNM content values assigned to receipts by the originators.

J. *What Would an MC&A Detection and Response Program Involve?*

The focus would be on rapidly detecting and responding to indications of SNM loss, including possible theft or diversion. This includes triggering investigations and resolving action on anomalies, as well as a way to thwart any attempts to covertly steal or divert SNM by insiders acting individually or in collusion. The design of measures to counter such a potential internal threat is to include a diversion path analysis or risk analysis of postulated scenarios considering conceivable ways and means potential insiders might try to steal or divert SNM at a GROA.

As background, the general diversion path analysis method that has been used by the NRC is described in the open literature (R. Hawkins, S. Baloga, N. Zack, W. Stanbro, and J. Markin, “Diversion Path Analysis - A New Approach,” INMM Proceedings XXI, 763-769, 1992). This technical paper expanded on diversion path analysis methods originally developed by the U.S. Bureau of Standards and published by the U.S. Energy Research and Development Administration (ERDA) (M. Maltese, K. Goodwin, and J. Scheter, “Diversion Path Analysis Handbook,” ERDA, October 1976). In addition, diversion path analysis methods have been extensively applied by the International Atomic Energy Agency (IAEA) for designing and implementing its safeguards strategy under the Treaty on the Non-Proliferation of Nuclear Weapons. Regarding the generic safeguarding of geologic repositories, the IAEA has published a comprehensive, multi-volume document (“Safeguards for the Final Disposal of Spent Fuel in Geologic Repositories,” STR-312, IAEA, Department of Safeguards, September 1998), which identifies and analyzes, in considerable detail, resulting diversion paths for a hypothetical facility.

K. *What Additional Requirements Would be Imposed if The DOE Possesses Formula Quantities of Strategic SNM that is in a Form Other than as Irradiated Nuclear Reactor Fuel?*

Additional requirements would be included for specified system capabilities for strategic SNM. These requirements include additional measures for item monitoring and more rigorous access control, quality assurance, and alarm resolution in concert with any enhanced physical protection to be provided under 10 CFR Part 73.

L. *What Special MC&A-Related Needs Exist?*

There is a need to consider risk-informed, performance-based alternatives for resolving anomalies, particularly onsite NDA measurements by The DOE in cases where item identity and integrity may have been compromised. Another need is the extent of item control and

physical inventorying that would be necessary for SNM (in HLW and other radioactive waste) in underground drifts and at aging pads, especially from a containment, surveillance, and access control perspective, and a worker perspective that involves reducing radiation exposure to personnel to as low as is reasonably achievable, as well as other impact aspects. The MC&A plan also needs to address SNM control and accounting functional aspects of retrievability and alternate storage capabilities that are required by §§ 60.21(c)(12) and 63.21(c)(7).

M. *What is the Objective of the Proposed Physical Security Requirements?*

The objective of the proposed physical security requirements is to provide high assurance that activities at a GROA are not inimical to the common defense and security, and do not constitute an unreasonable risk to the public health and safety. In order to provide a high assurance of protection, the NRC's philosophy is to use a defense-in-depth strategy towards the protection of HLW. Defense-in-depth relies on a holistic approach towards the protection of these materials and other radioactive materials, which includes using people, processes, equipment, and facilities to protect HLW and other radioactive materials from theft or diversion or radiological sabotage for malevolent purposes. The GROA physical security requirements would be determined using a graded approach related to the projected risk from radiological sabotage, theft, or diversion of HLW and other radioactive materials.

N. *What Threat Would a GROA be Required to Defend Against?*

The design basis threat defined in § 73.1(a) would apply to a GROA in the specific circumstances where a radiological sabotage or theft and diversion event may involve formula quantities of SNM. Under the proposed rule, the threat to a GROA is largely defined by specific security scenarios which represent the greatest threats against which GROA security forces must be able to defend against, with a high assurance of success. A GROA would have graded security measures based on the material, waste form, and operations within a particular

facility at a GROA. Therefore, depending on the material content, quantity, and consequence from a radiological sabotage event, as well as the theft or diversion of certain material, the security measures may rely on the design basis threat defined in §73.1(a) or may rely on other Commission requirements.

O. *Why do the Security Requirements Differ for Various Aspects of a GROA*?

The consequences of radiological and theft or diversion security events are highly dependent on the characteristics and packaging of the HLW and other radioactive materials and their location within a GROA. The activities and operations at a GROA aid in defining the physical security requirements and protective strategies that would be implemented. At this time, the GROA concept of operations has not been fully defined by the DOE; therefore, the NRC is establishing physical security requirements that would be dependent upon the consequences of a potential radiological event and the theft or diversion of certain material. These physical security requirements would be based on five proposed protection levels. The highest protection level would be for waste containing strategic SNM with the protection system designed to protect the material against the design basis threat for both theft or diversion and radiological sabotage. The next protection level would be for radioactive material that could result in a significant radiological sabotage event releasing radioactive materials in sufficient quantity such that any individual located at the lesser of the controlled area boundary or 400 meters from the source could receive a total effective dose equivalent equal to or greater than 0.25 Sv (25 rem). For these materials, the protection system must be designed to protect against the design basis threat for radiological sabotage. The third protection level would be for radioactive material that could result in a moderate radiological sabotage event releasing radioactive materials in sufficient quantity such that any individual located at the lesser of the controlled area boundary or 400 meters from the source could receive a total effective dose

equivalent equal to or greater than 0.05 Sv (5 rem) but less than 0.25 Sv (25 rem). For these materials, the protection system must be designed to protect the material against radiological sabotage. The fourth protection level would be for all other radioactive material containing SNM. The physical protection system would be designed to protect the material against security-related events specified for theft and diversion. The lowest protection level would be for other solidified radioactive material and material that would meet the criteria in Appendix P to 10 CFR Part 110 (Categories 1 and 2 radioactive materials). The protective strategy for these materials would be equivalent to the increased controls (i.e., prevent or impede removal, locate and prompt recovery, and mitigation of any potential consequence).

P. *Would Access Authorization Requirements Apply to a GROA and What Would They Cover?*

Yes, access authorization requirements would apply to a GROA. The facilities that possess large radiation sources, such as irradiated nuclear reactor fuels (e.g., SNF), are attractive targets for those who seek to commit radiological malevolent acts. Insiders who have unescorted access to facilities that possess such radiation sources, including a GROA, could pose a threat to the public health and safety or the common defense and security because they may have the ability to commit radiological malevolent acts. Therefore, imposing access authorization requirements is a prudent security measure to ensure that individuals who are granted unescorted access to the protected area of a GROA: (1) are trustworthy and reliable; (2) do not impose an unreasonable risk to the health and safety of the public or the common defense and security (as a result of increasing the likelihood of an insider threat); and (3) do not pose a potential threat to commit radiological malevolent acts or theft or diversion of HLW. Fingerprints are required of any individual granted unescorted access to the protected area of a GROA.

Q. *Would Criminal History Checks Apply to a GROA?*

Section 652 of the EPAct amended Section 149 of the AEA to require fingerprinting and a Federal Bureau of Investigation identification and criminal history records check of any person who is permitted unescorted access to radioactive materials subject to regulation by the Commission, and which the Commission determines to be of such significance to the public health and safety or the common defense and security as to warrant fingerprinting and background checks. The Commission has determined that the radioactive material at a GROA is of such significance and is proposing to implement the requirement for fingerprinting and a FBI identification and criminal history records check of any person who is permitted unescorted access to radioactive materials at a GROA. Background investigations, which include criminal history checks, represent a key element of the access authorization program ensuring that individuals who have unescorted access to a GROA are trustworthy and reliable. To accomplish this task, requirements were developed that focused on accumulating data on an individual's past that would produce an overall perspective of the individual's character and allow the licensee to make a determination of trustworthiness and reliability.

R. *What are the Key Aspects of the Security Requirements?*

The key aspects of the security requirements for a GROA are similar to the security requirements for similar types of NRC-licensed material and facilities. The proposed regulations would require an integrated security plan that would implement defense-in-depth concepts and protective strategies based on protecting target sets from various threat scenarios. The requirements are performance based and include an access authorization program and a physical protection system to detect, delay, and respond to postulated threat scenarios in such a way that prevents or mitigates undesirable consequences of malevolent actions. The postulated threat scenarios include the theft or diversion of SNM and HLW as well as radiological sabotage. The access authorization program requirements include measures

necessary to assure that personnel having critical safety or security functions or having access to certain nuclear materials remain trustworthy and reliable. The physical protection system requirements for detection measures include intrusion sensing, alarm communication, alarm assessment, and entry or access controls. Detection would be provided through the use of detection equipment, patrols, access controls, and other program elements required by this proposed rule. It also would provide notification to the licensee that a potential threat is present and where the threat is located. Alarm assessment is the mechanism through which the licensee obtains the information necessary to identify the nature of the threat detected and to determine how to respond. There are access control requirements for personnel, vehicles, and hazardous materials. The requirements for delay measures include barriers to delay adversarial actions to allow a timely response by security personnel. The requirements for responding to malevolent events allow the DOE to develop effective response strategies to challenge intruders so they cannot accomplish actions that are necessary to achieving undesirable consequences. In some instances, the strategy may include neutralizing adversaries to deny access to the nuclear material. The proposed rule uses a risk-informed approach for response requirements that permits protective strategies to be tailored to the type of material being protected, operations that involve handling this material and the potential consequences of postulated threat scenarios.

Security personnel who are responsible for the protection of the radioactive waste would be required to meet minimum requirements and performance criteria. The DOE would have to meet general criteria requirements for selection, training, equipping, testing, qualification, and contingency plans of security forces involved in GROA operations. These requirements would include hiring personnel who function as drill and exercise controllers to ensure that security forces are trained and qualified to execute their assigned duties. Drills and exercises are key

elements to assuring the preparedness of the security force and must be conducted in a manner that demonstrates the DOE's ability to execute the protective strategy as described in the site security plans. As for contingency plans, the information required in the safeguards contingency plans includes responses to threats, up to and including design basis threats, as described in § 73.1(a). The DOE would be required to submit for NRC approval a plan detailing how the prescribed criteria are going to be met.

S. *What is a Target Set as it Applies to a GROA?*

As it applies to a GROA, 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 operational disruption or radiological contamination barring extraordinary action by site operators. For a GROA, a target set means the quantities and form of HLW and other radioactive material and the protective and mitigative measures to protect against potential large scale releases of fission products from malevolent actions. For example, a target set with respect to spent fuel sabotage at a GROA could be 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. Due to the sensitivity of this information, specific target sets to the GROA will not be available in a public document.

T. *What Weapons Authorization Would be Necessary for the GROA Operations?*

There are two ways weapons may be authorized for use at a GROA. First, section 161A of the AEA allows the NRC to authorize licensees to use, as part of their protective strategies, an expanded arsenal of weapons, including machine guns. Section 161A was added to the AEA under the EPAct. Secondly, under section 161k. of the AEA, the DOE has separate authority for authorization of weapons on any of its sites. The DOE, under its own authority under section 161k. of the AEA, may authorize the use of an expanded weapons arsenal,

limited arrest authority, and the use of force in accordance with the DOE's current regulations under 10 CFR Part 1047. The NRC does not plan to use its authority under Section 161A of the AEA.

U. *Would DOE be Required to Conduct Force-on-Force Exercises for the GROA Facility?*

Yes, some type of force-on-force exercises are necessary to test the effectiveness of the DOE's protective strategies for the high-consequence target sets. The requirement for annual force-on-force exercises only applies to formula quantities of strategic SNM and significant radiological sabotage consequence target sets.

V. *How Would the Security Plans Handle Construction at a GROA After Receipt of HLW Begins?*

A license to receive and possess source, special nuclear, or byproduct material at a GROA may only be issued by the Commission on a finding that construction of the GROA has been substantially completed. Construction may be considered substantially complete if the construction of surface and interconnecting structures, systems, and components and any underground storage space required for initial operation are substantially complete. Some construction activities could continue once receipt of material begins.

The NRC's security requirements are designed to protect all material at a GROA. Handling, storage, and emplacement operations for HLW and other radioactive materials shall be conducted inside a protected area. The NRC's security requirements are flexible enough to allow the DOE to establish a protected area that could separate remaining construction activities from operations involving HLW and other radioactive material. Any construction activity occurring within the protected area would be subject to the NRC's security requirements. Any construction activities outside the protected area, but within the DOE controlled area, would be subject to some NRC security controls and DOE security orders. The

protected area and security plans would be expanded to include new facilities or areas before radioactive material could be received in that new facility or area.

W. *Does this Rulemaking Cover Transportation of High-Level Radioactive Waste to a GROA?*

No, the NRC's regulatory authority is limited to the operations at a GROA. As an independent Federal Agency, the DOE must comply with its own internal requirements (DOE orders) and Departments of Transportation and Homeland Security regulations when transporting HLW and other radioactive materials to a GROA. However, the DOE must use shipping containers certified by the NRC under the regulations in 10 CFR Part 71. Part 71 is not being revised by this proposed rule.

X. *Would the Security and MC&A Plans Cover Postclosure?*

No, these plans would not cover the postclosure period. Once the NRC license is terminated, the NRC would no longer have regulatory authority. However, the DOE plans for continued oversight of the Yucca Mountain site after permanent closure.

Y. *What Safeguards Reporting Requirements Would be Proposed for a GROA?*

Prompt notification to the NRC of a security event involving an actual or imminent threat would permit the NRC to contact other Federal authorities and other licensees, as appropriate. The Commission would expect the DOE to notify the NRC Operations Center as soon as possible after they notify local law enforcement agencies, but within 15 minutes. A written 60-day report would also be required for these notifications. This new reporting requirement would require the DOE to promptly notify the NRC of any event involving an actual or imminent threat at the GROA.

Four-hour notification would be proposed for suspicious activities, attempts at access, etc., that may indicate pre-operational surveillance, reconnaissance, or intelligence gathering activities targeted against the GROA. This would assist the intelligence and homeland security

communities in evaluating threats across critical infrastructure sectors.

The current provision for one-hour notifications for certain safeguards events (e.g., theft or unlawful diversion of SNM, significant physical damage to the facility, entry of an unauthorized person into protected areas) would be retained, with some modifications to include attempted actions and to broaden the scope of the language used for specific areas. The provision for events to be recorded in the safeguards log would also be retained.

Z. *Does the NRC Plan to Issue Guidance Documents?*

Yes, the NRC intends to issue guidance documents. The NRC intends to issue a GROA-specific regulatory guidance document. This document would address adversary characteristics for the design basis threats and describe details of the GROA security-related threats. Other guidance documents are under consideration. The publication of the guidance documents is planned after the publication of the final rule. Because the guidance documents may contain Safeguards Information and/or classified information, these documents would only be available to those with a need-to-know, and who are qualified to have access to Safeguards Information 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.

AA. *Would the GROA Facilities be Subject to IAEA Safeguards?*

The U.S. Government has not yet made a determination as to whether a GROA can be subject to IAEA safeguards.

BB. *What Changes Would be Made to the Emergency Plan Requirements?*

The emergency plan requirements would be changed to reflect the need to respond to radiological emergencies instead of radiological accidents. The term radiological emergencies is more inclusive of the types of situations that the emergency plan may need to address. In

addition, § 63.21(c)(21) requires a description of the plan for responding to, and recovering from, radiological emergencies; the proposed change is consistent with this language.

CC. *What Should I Consider as I Prepare My Comments to NRC?*

Tips for preparing your comments - when submitting your comments, remember to:

i. Identify the rulemaking (RIN 3150-AI06).

ii. Explain why you agree or disagree; suggest alternatives and substitute language for your requested changes.

iii. Describe any assumptions and provide any technical information and/or data that you used.

iv. If you estimate potential costs or burdens, explain how you arrived at your estimate in sufficient detail to allow for it to be reproduced.

v. Provide specific examples to illustrate your concerns, and suggest alternatives.

vi. Explain your views as clearly as possible.

vii. Make sure to submit your comments by the comment period deadline identified.

viii. See Section VI of the preamble for the request for comments on the use of plain language and Section XI for the request for comments on the draft regulatory analysis.

III. Discussion of Proposed Amendments by Section

Section 60.21 Content of application.

Paragraph (b)(3) would be revised to change the reference for the security requirements from § 73.51 to the new requirements in § 73.53 and to require a description instead of plans. Paragraph (b)(4) would be revised to change the reference for the MC&A requirements from § 60.78 to the new requirements in 10 CFR Part 74. The actual plans would be submitted after

the construction authorization was issued. The security and MC&A plans would not be implemented until SNM is received at the GROA.

Section 60.24 Updating of application and environmental impact statement.

Paragraph (d) would be added to require the DOE to submit the actual security plans and MC&A plan for NRC approval no later than 180 days after the Commission issues the construction authorization. Under the current regulations, the DOE was not required to submit the actual MC&A plan for NRC approval. This requirement corrects that oversight.

Section 60.78 Criticality reporting.

This section would be renamed to reflect the criticality reporting that remains after the MC&A requirements are relocated to 10 CFR Part 74. Currently, the criticality reporting requirement is captured by the reference to § 72.74. The section would be revised to include the criticality reporting requirement instead of a reference to another section. The actual requirements would not change.

Section 63.21 Content of application.

Paragraph (b)(3) would be revised to change the reference for the security requirements from § 73.51 to the new requirements in § 73.53 and would clarify that only a description of the program need be submitted with the construction application. Paragraph (b)(4) would be revised to change the reference for the MC&A requirements from § 63.78 to the new requirements in 10 CFR Part 74. The actual security and MC&A plans would be submitted after the construction authorization was issued. The security and MC&A plans would not be implemented until SNM is received at the GROA.

Section 63.24 Updating of application and environmental impact statement.

Paragraph (d) would be added to require the DOE to submit the actual security plans and MC&A plan for NRC approval no later than 180 days after the Commission issues the construction authorization. Under the current regulations, the DOE was not required to submit the actual plans for NRC approval. This requirement corrects that oversight.

Section 63.78 Criticality reporting.

This section would be renamed to reflect the criticality reporting that remains after the MC&A requirements are relocated to 10 CFR Part 74. Currently, the criticality reporting requirement is captured by the reference to § 72.74. The section would be revised to include the criticality reporting requirement instead of a reference to another section. The actual requirements would not change.

Section 63.161 Emergency plan for the geologic repository operations area through permanent closure.

This section would be revised to refer to radiological emergencies instead of radiological accidents. The term radiological emergencies is more inclusive of the types of situations that the emergency plan may need to address. In addition, § 63.21(c)(21) requires a description of the plan for responding to, and recovering from, radiological emergencies; the proposed change is consistent with that language. The reference to develop and implement a plan to "cope with radiological accidents" is changed to a plan to "provide reasonable assurance that adequate protective measures can and would be taken in the event of a radiological emergency."

Section 73.2 Definitions.

This section would be revised to incorporate the definition for high-level radioactive waste in 10 CFR Part 63 and to add a definition for target set for application to a GROA.

Section 73.50 Requirements for physical protection of licensed activities.

This section would be revised to include a reference to § 73.53 to retain the exemption for a GROA from the security requirements listed in the section. Requirements for a GROA are specified in proposed § 73.53.

Section 73.51 Requirements for physical protection of stored spent nuclear fuel and high-level radioactive waste.

This section would be revised to remove references to a GROA. The security requirements for an ISFSI and a monitored retrievable storage installation would remain unchanged. The requirements for a GROA would be contained in new section § 73.53.

Section 73.53 Requirements for physical protection at a geologic repository operations area.

The proposed rule would create a new section for the GROA physical protection requirements. The existing requirements for GROA security are contained in § 73.51(b), (c), and (d). The requirements have been expanded and strengthened to reflect the post-September 11, 2001, threat environment and placed in this new section.

Paragraph (a) would establish that the physical protection requirements in this section apply to The DOE for the operation of a GROA.

Paragraph (b)(1) would require The DOE to submit a Physical Security Plan, Training

and Qualification Plan, and Safeguards Contingency Plan that describe how the requirements of the section would be met. The plans would be submitted no later than 180 days after the NRC issues a construction authorization for a GROA. Paragraph (b)(1) would also establish the implementation timeframe. Paragraph (b)(2) would exempt the DOE from the security requirements after permanent closure of a GROA. This provision is currently located at § 73.51(e).

Paragraph (c) would establish the performance objectives. Paragraph (c)(1) would establish the general performance objective to provide high assurance that activities involving radioactive waste are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. The current general objective does not address common defense and security. Paragraphs (c)(2) and (c)(3) would establish objectives based on the type and form of material and the consequences of a postulated radiological sabotage event. The more risk-significant the material, the higher the level of protection required.

Paragraph (d) would establish general requirements for the physical security program. The DOE would be required to design and implement a program to satisfy the performance requirements and to ensure that no single act can disable the personnel, equipment, or systems necessary to prevent the theft of strategic SNM and significant radiological sabotage. The DOE would also be required to establish and maintain a written performance evaluation program, an access authorization program, an insider mitigation program, and a corrective action program.

Paragraph (e) would require the DOE to develop security plans that describe how the physical protection program would prevent the theft or diversion and radiological sabotage of SNM and byproduct material and to protect safeguards information against unauthorized

disclosure. The DOE would be required to establish, implement, and maintain written procedures and to have a process for the DOE's approval of implementing procedures. The DOE would be allowed to make changes to the security plans without NRC approval as long as the changes do not decrease the plan's effectiveness. The DOE would be required to establish, maintain, and follow a Commission-approved training and qualification plan and a safeguards contingency plan and to establish, implement, and maintain a Commission-approved physical security plan.

Paragraph (f) would require the DOE to 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. The Commission expectation would be that the management system oversee all aspects of the onsite physical protection program to ensure the effective implementation of Commission requirements through the approved security plans and implementing procedures. The DOE would also be required to ensure that any written agreement with any contractor used to implement the onsite physical protection program was retained as a record for the duration of the contract and that the contract clearly state several conditions related to training, access authorization, and document availability. Provisions regarding the security organization are currently addressed at § 73.51(d)(5). The proposed requirements would strengthen and expand on the current requirements.

Paragraph (g) would provide a performance-based requirement for determining the use and placement of physical barriers for the protection of personnel, equipment, and systems, the failure of which could directly or indirectly endanger public health and safety. The DOE would be required to establish and maintain physical barriers in the controlled area, as necessary, to deter, delay, or prevent unauthorized access; facilitate the early detection of unauthorized activities; and control approach routes to the facility. Paragraph (g) would establish

requirements related to physical barriers (paragraph (g)(3)), isolation zones (paragraph (g)(4)), protected areas (paragraph (g)(5)), vital areas (paragraph (g)(6)), vehicle barrier systems (paragraph (g)(7)), and unattended openings (paragraph (g)(8)). Current provisions addressing physical barriers are located at § 73.51(d)(1). The proposed requirements would strengthen and expand on the current requirements.

Paragraph (h) would require the DOE to develop and identify target sets and document the analyses and methodologies used to determine and group the target set equipment or elements. The DOE would also be required to implement a program for the oversight of certain facility equipment and systems documented as part of the the DOE protective strategy.

Paragraph (i) would require The DOE to establish an access control program for personnel, vehicles, and material. The paragraph would establish the features required for the access control program, including access control points, emergency conditions, vehicles, access control devices, visitors, and escorts. Current provisions addressing access control are found at § 73.51(b)(2), 73.51(d)(7), and 73.51(d)(9). The proposed requirements would strengthen and expand on the current requirements.

Paragraph (j) would establish the requirements for search programs for individuals, packages, and vehicles. This paragraph would expand and strengthen the current requirements located in § 73.51(d)(9).

Paragraph (k) would establish the requirements for the detection and assessment systems. The DOE would be required to establish and maintain an intrusion detection and assessment system that must provide the capability for early detection and assessment of unauthorized persons and activities. This proposed requirement would not mandate specific intrusion detection equipment for any specific area, but rather would require that the system provide detection and assessment capabilities that meet Commission requirements. The

current requirements addressing detection and assessment systems are located at § 73.51(b)(2), 73.51(d)(2), 73.51(d)(3), 73.51(d)(4), and 73.51(d)(11). The proposed requirements would strengthen and expand on the current requirements.

Paragraph (l) would require the DOE to establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations. The chosen communication method would be available and operating any time it would be needed to communicate information. The proposed requirements would strengthen and expand on the current requirements located at § 73.51(b)(2), 73.51(d)(6), and 73.51(d)(8).

Paragraph (m) would establish the response requirements for personnel and equipment and armed responders. The DOE would be required to establish and maintain the minimum number of properly trained and equipped personnel required to intercept, challenge, delay and/or neutralize any security related events.

Paragraph (n) would require the DOE to implement a cyber-security program that provides high assurance that computer systems, which if compromised could adversely impact safety, security, and emergency preparedness, are protected from cyber attacks.

Paragraph (o) would establish the requirements for security program reviews and audits. The DOE would be required to review the physical protection program at intervals not to exceed 12 months or as necessary based upon assessments or other performance indicators with each element being reviewed at least every 24 months. The DOE would also be required to conduct quarterly drills and annual exercises in accordance with Section III of Appendix C of 10 CFR Part 73 and the The DOE performance evaluation program. The proposed requirements expand on the current requirement for a physical protection program review every 24 months that is in § 73.51(d)(12).

Paragraph (p) would require the DOE to implement a maintenance, testing and calibration program to ensure that security programs 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.

Paragraph (q) would require the DOE to 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.

Paragraph (r) would authorize the DOE to suspend implementation of affected requirements of § 73.53 in an emergency when action is immediately needed to protect the public health and safety and during severe weather when the suspension is needed to protect personnel from a life threatening situation. In both cases, a designated senior site manager would need to approve the suspension before taking the action.

Paragraph (s) would require the DOE to maintain all records required to be kept until the Commission terminates the license and to maintain superseded portions of these records for at least 3 years after the record is superseded.

Paragraph (t) would require the DOE to develop and implement a process to inform and coordinate safety and security activities to ensure that these requirements do not adversely affect the capabilities of the security organization to satisfy the security requirements or overall GROA safety.

Paragraph (u) would provide a mechanism for the DOE to receive approval for use of alternative measures to those required by § 73.53. Current provisions for alternative measures are covered by § 73.51(d).

Paragraph (v) would contain additional performance capabilities that must be met if the DOE were to possess formula quantities of strategic SNM, unless otherwise approved by the

Commission. These additional measures include requirements on the security organization; physical barrier subsystem; access control subsystem and procedures; search programs; detection, surveillance, and alarm subsystems and procedures; and response requirements.

Section 73.56a Personnel access authorization requirements for a geologic repository operations area.

This section would be added to address the requirements for the personnel access authorization program for a GROA. The current regulations require the DOE to grant access to the protected area only to individuals who are authorized to enter the protected area; however, there are no specific requirements for the access authorization program. The proposed program addresses the integration of the access authorization requirements and security program requirements. The proposed performance objective is to provide high assurance that individuals granted unescorted access 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, theft, or diversion. The proposed rule would establish requirements for the background investigation (paragraph (d)), psychological assessments (paragraph (e)), behavioral observation (paragraph (f)), arrest reporting (paragraph (g)), granting unescorted access authorization (paragraph (h)), maintaining access authorization (paragraph (i)), access to vital areas (paragraph (j)), trustworthiness and reliability of background screeners and authorization program personnel (paragraph (k)), review procedures (paragraph (l)), protection of information (paragraph (m)), audits and corrective action (paragraph (n)), and records (paragraph (o)). The proposed requirements are nearly identical as those proposed for power reactors (71 FR 62664; October 26, 2006).

Section 73.57 Requirements for criminal history checks of individuals granted unescorted access to a nuclear power facility or the protected area of a geologic repository operations area, or access to Safeguards Information by power reactor licensees.

This section would be retitled to include the protected area of a GROA. New paragraph (a)(4) would be added to require the DOE to comply with the requirements for criminal history checks contained in this section upon receipt of Commission authorization to receive and possess source, special nuclear, or byproduct material at a GROA. Paragraph (b)(2)(iii) would be added to expand the requirements for criminal history checks to anyone granted unescorted access to the protected area of a GROA. Paragraphs (b)(1), (b)(4), (b)(4)(i), (b)(5), (b)(8), (c)(1), (d)(1), (f)(2), and (f)(5) would be revised to expand the requirements to individuals granted unescorted access to the protected area of a GROA.

Section 73.70 Records.

The introductory paragraph would be revised to include a reference to § 73.53. Paragraph (c)(1) would be added to include a reference to § 73.53(i)(7). A new paragraph (c)(1) is being proposed because changes to paragraph (c) have been proposed in the power security rule and it could cause confusion to stakeholders to propose additional changes to the same section. This section would establish the requirements for record retention. Record retention requirements are currently located in § 73.51(c), 73.51(d)(10), and 73.51(d)(13). The record retention period remains 3 years or termination of the license, depending on the record type.

Section 73.71a Reporting of safeguards events for a GROA.

Section 73.71a would be created to contain the safeguards reporting events that are

specific to a GROA. A new section is being proposed because significant changes to this section have been proposed in the power reactor security rule and it could cause significant confusion to stakeholders to propose additional changes to the same section. A new reporting requirement is proposed that would require the DOE to promptly notify the NRC of any event involving an actual or imminent threat. Four-hour notification is being proposed for suspicious events and tampering events not otherwise covered under Appendix G. The provision for one-hour notifications for certain safeguards events (e.g., theft or unlawful diversion of SNM, significant physical damage to any facility, entry of an unauthorized person into protected areas.) would be retained, with some modifications to include attempted actions and to broaden the scope of the language used for specified areas. The provisions for events to be recorded in the safeguards log would be retained with minor revisions. Requirements for making the required telephonic and written notifications are also proposed.

Appendix B to 10 CFR Part 73 - General Criteria for Security Personnel.

A new Section VII, “Geologic Repository Operations Area Training and Qualification Plan,” would contain the training and qualification requirements for security personnel. These new requirements would include additional physical requirements for unarmed security personnel to assure the 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.

Appendix C to 10 CFR Part 73 - Licensee Safeguards Contingency Plans.

A new Section III, “Geologic repository operations area safeguards contingency plans,” would establish the requirements that govern the development of the safeguards contingency plan for a GROA. Proposed requirements include 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 GROA security force and must be conducted in a manner that demonstrates the DOE’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 facility safety.

Appendix G to 10 CFR Part 73 - Reportable Safeguards Events.

The introductory paragraph would be revised to include a reference to §§ 73.71a and 73.53 to address the reporting provisions that would apply specifically to a GROA. The reporting requirements would be revised to support the revised reporting requirements from proposed § 73.71a. Paragraph V would be added to require prompt reporting (not later than 15 minutes of discovery) after the discovery of an imminent or actual threat against the facility. Paragraph VI would contain the reports to be reported within one (1) hour. Paragraph VII would contain the events to be reported with four (4) hours. Paragraph VIII would contain the events to be recorded in the safeguards log.

Section 74.1 Purpose.

Paragraph (b) would be revised to include a reference to §§ 60.21 and 63.21 to cover submittal of a license application for a GROA.

Section 74.2 Scope.

Paragraph (b) would be revised to include a reference to the proposed Subpart F.

Section 74.4 Definitions.

This section would be revised to add definitions for accounting, custodian, high-level radioactive waste, item control area, item control program, and material balance area.

Section 74.13 Material Status Reports.

Paragraph (a) would be revised to require the submittal of Material Status Reports within 60 calendar days of the GROA physical inventory. This requirement was previously covered by § 72.76.

Section 74.17 Special nuclear material physical inventory summary report.

Paragraph (d) would be added to require the DOE to submit Special Nuclear Material Physical Inventory Summary Reports for the GROA.

Section 74.19 Recordkeeping.

Paragraphs (a) and (c) would be revised to exempt a GROA from the recordkeeping requirements because the recordkeeping requirements for a GROA would be specified in a new Subpart F.

Subpart F - Geologic Repository Operations Area

This new subpart would contain the MC&A requirements that are specific for a GROA.

The new Subpart would contain requirements that are both risk informed and performance based.

Section 74.71 Nuclear material control and accounting for a geologic repository operations area (GROA).

This new section would contain the MC&A general performance objectives (paragraph (a)), the systems capabilities (paragraph (b)), and the implementation dates (paragraph (c)) for a GROA. Required systems capabilities and features would be commensurate with the kind, amount, and specifications of the SNM proposed to be possessed at a GROA.

Paragraph (a) would require the DOE to establish, implement, and maintain a Commission-approved MC&A program that meets the following performance objectives: (1) maintain accurate, current, and reliable information on, and confirm the quantities and locations of, SNM; (2) detect, respond to, and resolve any anomalies indicating a possible loss of SNM; (3) permit rapid determination of whether an actual loss of a significant amount of SNM has occurred: (4) generate and provide, as requested, information to aid in the investigation and recovery of missing SNM; and (5) control access to MC&A information that might assist adversaries in possible attempts to carry out a theft or diversion, or to help target HLW for radiological sabotage.

Paragraph (b) would require the DOE to include the capabilities and features specified in Section 74.73 in the MC&A program.

Paragraph (c) would require the DOE to submit an MC&A plan that describes how the performance objectives would be achieved and the system capabilities would be met. The plan would be submitted no later than 180 days after the NRC issues a construction authorization for the GROA. Paragraph (c) would also require the DOE to implement the Commission-approved

MC&A plan upon issuance of a license to receive and possess source, special nuclear, or byproduct material at the GROA or by a date specified in a license condition.

§ 74.73 Internal controls, inventory, and records.

This new section would establish the internal controls (paragraphs (b), (c), (d), (e), (f), (g), and (h)), inventory requirements (paragraph (i)), additional provisions for receipt of strategic SNM (paragraph (j)), and the recordkeeping requirements (paragraph (k)) for the MC&A program.

Paragraph (a) would require the DOE to establish and maintain the internal control, inventory, and recordkeeping capabilities that would be required by paragraphs (b) through (k).

Paragraph (b) would require the DOE to establish, document, and maintain a management structure that assures clear overall responsibility for the MC&A program, would be independent of other operations, and would provide for separation of key responsibilities. The DOE would also be required to provide for the adequate review, approval, and use of written procedures.

Paragraph (c) would require the DOE to assure that personnel that work in key positions are trained to maintain a high-level of safeguards awareness and are qualified to perform their duties.

Paragraph (d) would require the DOE to perform and document independent reviews and assessments of the total MC&A program at intervals not to exceed 24 months.

Paragraph (e) would require the DOE to establish, document, implement, and maintain an item control program that: (1) provides current knowledge of all HLW items with respect to unique identity, element and isotope content, and location from receipt to underground emplacement and possible retrieval and alternate storage; (2) assures that the integrity of items

is maintained such that the unauthorized removal of SNM would be readily apparent; (3) maintains and follows procedures for any tamper-safing program that is to be used for assuring the validity of prior measurements; and (4) stipulates the use of the 2-person rule for sealing operations, affixing tamper-indicating devices, handling of bare fuel assemblies, performing physical inventories, and internal transfers.

Paragraph (f) would require the DOE to establish, implement, and maintain an anomaly, detection, and response program that incorporates checks and balances sufficient to thwart attempts to divert SNM and to detect falsification of data and reports that could conceal the theft or diversion of SNM. The program would also be required to detect and respond to a potential loss or misuse of SNM, including the theft or diversion of SNM by an internal threat using collusion, stealth, and deceit. The overall design of the detection and response program would need to include an analysis of conceivable ways and means through which clandestine attempts of theft, diversion, or other misuse might occur.

Paragraph (g) would require the DOE to establish, document, implement, and maintain a program to reasonably assure the validity of assigned SNM quantities, including a measurement system and a measurement control program that maintains a level of effectiveness sufficient to satisfy the capabilities required for resolving anomalies, as needed.

Paragraph (h) would require the DOE to provide information to the NRC or other agencies deemed necessary for conducting an investigation of actual (or highly suspected) events pertaining to missing SNM and information relevant to recovery of the SNM.

Paragraph (i) would require the DOE to perform a facility-wide physical inventory of all possessed SNM to close material balances at intervals not to exceed 12 calendar months. The paragraph would further require the DOE to provide written instructions for conducting the physical inventories. Within 60 days after the start of the inventory, the DOE would be required

to reconcile and adjust the book record, as appropriate, to the results of the physical inventory and to investigate and resolve, or report any unresolved inventory difference or discrepancy to the NRC.

Paragraph (j) would require the DOE to establish additional measures, if the DOE were to receive formula quantities of strategic SNM that are in a form other than irradiated reactor fuel or high-level radioactive waste. These additional measures include: (1) item-monitoring features as specified in § 74.55; (2) alarm resolution as specified in § 74.57; (3) quality assurance and accounting capabilities as specified in § 74.59; (4) establishment of controlled areas for strategic SNM; and (5) semi-annual physical inventories of all strategic SNM.

Paragraph (k) would require the DOE to establish records that demonstrate that the requirements have been met, to maintain the records in duplicate in an auditable form, and to retain the records until the Commission terminates the GROA license. The paragraph also requires the DOE to retain procedures until the Commission terminates the license, with superceded portions of a procedure to be retained for 3 years after the portion is superceded. The DOE would also be required to maintain adequate safeguards against tampering with and loss of records. The DOE must also satisfy the requirements of 10 CFR 60.71 or 63.71 for records on the receipt, handling, and disposition of radioactive waste at a GROA.

IV. Criminal Penalties

For the purpose of Section 223 of the Atomic Energy Act (AEA), as amended, the Commission is proposing to amend 10 CFR Parts 60, 63, 73, and 74 under one or more of 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 §§ 73.53, 73.56a, and 73.71a are issued under

Sections 161b, 161i, or 161o of the AEA, and are not included in § 73.81(b). Criminal penalties, as they apply to regulations in Part 74, are discussed in § 74.84. The new §§ 74.71and 74.73 are issued under Sections 161b, 161i, or 161o of the AEA, and are not included in § 74.84(b). Willful violations of the rule would be subject to criminal enforcement.

V. Agreement State Compatibility

Under the "Policy Statement on Adequacy and Compatibility of Agreement State Programs" approved by the Commission on June 30, 1997, and published in the Federal Register on September 3, 1997 (62 FR 46517), this rule is classified as Compatibility Category "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 Atomic Energy Act of 1954, as amended, or the provisions of Title 10 of the Code of Federal Regulations.

VI. Plain Language

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

VII. 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 the use of such a standard is inconsistent with applicable law or otherwise impractical. In this proposed rule, the NRC would establish security and MC&A requirements for a GROA. This action does not constitute the establishment of a standard that establishes generally applicable requirements.

VIII. Finding of No Significant Environmental Impact

Pursuant to Section 121(c) of the Nuclear Waste Policy Act, this proposed rule does not require the preparation of an environmental impact statement under Section 102(2)(c) of the National Environmental Policy Act of 1969 or any environmental review under subparagraph (E) or (F) of Section 102(2) of such act.

IX. Paperwork Reduction Act Statement

The information collection requirements contained in this proposed rule of limited applicability affect one respondent, which is a federal entity. Therefore, Office of Management and Budget approval is not required pursuant to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.).

X. 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.

XI. 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 comment on the draft regulatory analysis. Comments on the draft analysis may be submitted to the NRC as indicated under the ADDRESSES heading. The analysis is available for inspection in the NRC Public Document Room, 11555 Rockville Pike, Rockville, MD 20852.

XII. Regulatory Flexibility Certification

In accordance with the Regulatory Flexibility Act of 1980 (5 U.S.C. 605(b)), the Commission certifies that this rule would not, if promulgated, have a significant economic impact on a substantial number of small entities. This proposed rule affects only the licensing of one entity, the DOE, which does not fall within the scope of the definition of "small entities" set forth in the Regulatory Flexibility Act or the size standards established by the NRC (10 CFR 2.810).

XIII. Backfit Analysis

The NRC has determined that the backfit rule (§§ 50.109, 70.76, 72.62, or 76.76) does

not apply to this proposed rule because this amendment would not involve any provisions that would impose backfits as defined in 10 CFR Chapter I. Therefore, a backfit analysis is not required.

List of Subjects

10 CFR Part 60

Criminal penalties, High-level waste, Nuclear materials, Nuclear power plants and reactors, Reporting and recordkeeping requirements, Waste treatment and disposal.

10 CFR Part 63

Criminal penalties, High-level waste, Nuclear power plants and reactors, Reporting and recordkeeping requirements, Waste treatment and disposal.

10 CFR Part 73

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

10 CFR Part 74

Accounting, Criminal penalties, Hazardous materials transportation, Material control and accounting, Nuclear materials, Packaging and containers, Radiation protection, Reporting and recordkeeping requirements, Scientific equipment, Special nuclear material.

For the reasons set out in the preamble and under the authority of the Atomic Energy

Act of 1954, as amended; the Energy Reorganization Act of 1974, as amended; and 5 U.S.C. 552; the NRC is proposing to adopt the following amendments to 10 CFR Parts 60, 63, 73, and 74:

PART 60 -DISPOSAL OF HIGH-LEVEL RADIOACTIVE WASTES IN GEOLOGIC REPOSITORIES

1. The authority citation for Part 60 continues to read as follows:

AUTHORITY: Secs. 51, 53, 62, 63, 65, 81, 161, 182, 183, 68 Stat. 929, 930, 932, 933, 935, 948, 953, 954, as amended (42 U.S.C. 2071, 2073, 2092, 2093, 2095, 2111, 2201, 2232, 2233); secs. 202, 206, 88 Stat. 1244, 1246 (42 U.S.C. 5842, 5846); secs. 10 and 14, Pub. L. 95-601, 92 Stat. 2951 (42 U.S.C. 2021a and 5851); sec. 102, Pub. L. 91-190, 83 Stat. 853 (42 U.S.C. 4332); secs. 114, 121, Pub. L. 97-425, 96 Stat. 2213g, 2228, as amended (42 U.S.C. 10134, 10141), and Pub. L. 102-486, sec. 2902, 106 Stat. 3123 (42 U.S.C. 5851); sec. 1704, 112 Stat. 2750 (44 U.S.C. 3504 note).

2. In § 60.21, paragraphs (b)(3) and (b)(4) are revised to read as follows:

§ 60.21 Content of application.

* * * * *

(b) ***

(3) A description of the security measures for physical protection of high-level radioactive waste and other radioactive material in accordance with § 73.53 of this chapter. This description must include a description of the design for physical protection, the safeguards

contingency plan, and security organization personnel training and qualification plan. The description must list tests, inspections, audits, and other means to be used to demonstrate compliance with such requirements.

(4) A description of the material control and accounting program to meet the requirements of §§ 74.11, 74.13, 74.15, 74.17, 74.71, and 74.73 of this chapter.

* * * * *

3. In § 60.24, paragraph (d) is added to read as follows:

§ 60.24 Updating of application and environmental impact statement.

* * * * *

(d) DOE shall supplement its application no later than 180 days after the NRC issues a construction authorization for the GROA with the submittal of the following plans:

(1) Physical Security Plan;

(2) Training and Qualification Plan;

(3) Safeguards Contingency Plan; and

(4) Material Control and Accounting Plan.

4. Section 60.78 is revised to read as follows:

§ 60.78 Criticality reporting.

(a) DOE shall notify the NRC Operations Center[3] within one hour of discovery of any case of accidental criticality.

[3]Commercial telephone number of the NRC Operations Center is (301) 816-5100.

(b) This notification must be made to the NRC Operations Center via the Emergency Notification System if DOE is party to that system. If the Emergency Notification System is inoperative or unavailable, DOE shall make the required notification via commercial telephonic service or other dedicated telephonic system or any other method that will ensure that a report is received by the NRC Operations Center within one hour.

PART 63 - DISPOSAL OF HIGH-LEVEL RADIOACTIVE WASTES IN A GEOLOGIC REPOSITORY AT YUCCA MOUNTAIN, NEVADA

5. The authority citation for Part 63 continues to read as follows:

AUTHORITY: Secs. 51, 53, 62, 63, 65, 81, 161, 182, 183, 68 Stat. 929, 930, 932, 933, 935, 948, 953, 954, as amended (42 U.S.C. 2071, 2073, 2092, 2093, 2095, 2111, 2201, 2232, 2233); secs. 202, 206, 88 Stat. 1244, 1246 (42 U.S.C. 5842, 5846); secs. 10 and 14, Pub. L. 95-601, 92 Stat. 2951 (42 U.S.C. 2021a and 5851); sec. 102, Pub. L. 91-190, 83 Stat. 853 (42 U.S.C. 4332); secs. 114, 121, Pub. L. 97-425, 96 Stat. 2213g, 2238, as amended (42 U.S.C. 10134, 10141), and Pub. L. 102-486, sec. 2902, 106 Stat. 3123 (42 U.S.C. 5851); sec. 1704, 112 Stat. 2750 (44 U.S.C. 3504 note).

6. In § 63.21, paragraphs (b)(3) and (b)(4) are revised to read as follows:

§ 63.21 Content of application.

* * * * *

(b) ***

(3) A description of the security measures for physical protection of high-level

radioactive waste and other radioactive material in accordance with § 73.53 of this chapter. This description must include the description of the design for physical protection, the safeguards contingency plan, and security organization personnel training and qualification plan. The description must list tests, inspections, audits, and other means to be used to demonstrate compliance with such requirements.

(4) A description of the material control and accounting program to meet the requirements of §§ 74.11, 74.13, 74.15, 74.17, 74.71, and 74.73 of this chapter.

* * * * *

7. In § 63.24, paragraph (d) is added to read as follows:

§ 63.24 Updating of application and environmental impact statement.

* * * * *

(d) DOE shall supplement its application no later than 180 days after the NRC issues a construction authorization for the GROA with the submittal of the following plans:

(1) Physical Security Plan;

(2) Training and Qualification Plan;

(3) Safeguards Contingency Plan; and

(4) Material Control and Accounting Plan.

8. Section 63.78 is revised to read as follows:

§ 63.78 Criticality reporting.

(a) DOE shall notify the NRC Operations Center[3] within one hour of discovery of any case of accidental criticality.

(b) This notification must be made to the NRC Operations Center via the Emergency Notification System if DOE is party to that system. If the Emergency Notification System is inoperative or unavailable, DOE shall make the required notification via commercial telephonic service or other dedicated telephonic system or any other method that will ensure that a report is received by the NRC Operations Center within one hour.

9. Section 63.161 is revised to read as follows:

§ 63.161 Emergency plan for the geologic repository operations area through permanent closure.

DOE shall develop and be prepared to implement a plan to provide reasonable assurance that adequate protective measures can and will be taken in the event of a radiological emergency at the geologic repository operations area, at any time before permanent closure and decontamination or decontamination and dismantlement of surface facilities. The emergency plan must be based on the criteria of § 72.32(b) of this chapter.

PART 73 - PHYSICAL PROTECTION OF PLANTS AND MATERIALS

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

AUTHORITY: Secs. 53, 161, 68 Stat. 930, 948, as amended, sec. 147, 94 Stat. 780 (42 U.S.C. 2073, 2167, 2201); sec. 201, as amended, 204, 88 Stat. 1242, as amended, 1245, sec.

[3]Commercial telephone number of the NRC Operations Center is (301) 816-5100.

1701, 106 Stat. 2951, 2952, 2953 (42 U.S.C. 5841, 5844, 2297f); sec. 1704, 112 Stat. 2750 (44 U.S.C. 3504 note). Section 73.1 also issued under secs. 135, 141, Pub. L. 97-425, 96 Stat. 2232, 2241 (42 U.S.C, 10155, 10161). Section 73.37(f) also issued under sec. 301, Pub. L. 96-295, 94 Stat. 789 (42 U.S.C. 5841 note). Section 73.57 is issued under sec. 606, Pub. L. 99-399, 100 Stat. 876 (42 U.S.C. 2169) and under sec. 652, Pub. L. 109-58, 119 Stat 810 (42 U.S.C. 2169).

11. In § 73.2, definitions for *high-level radioactive waste* and *target set for a geologic repository operations area* are added in alphabetical order to read as follows:

§ 73.2 Definitions.

* * * * *

High-level radioactive waste or *HLW* means:

(1) The highly radioactive material resulting

from the reprocessing of spent nuclear fuel, including liquid waste produced directly in reprocessing and any solid material derived from such liquid waste that contains fission products in sufficient concentrations;

(2) Irradiated reactor fuel; and

(3) Other highly radioactive material that the Commission, consistent with existing law, determines by rule requires permanent isolation.

* * * * *

Target set for a geologic repository operations area 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 operational

disruption or radiological contamination barring extraordinary action by site operators. For a geological repository operations area (GROA), a target set means quantities and form of high-level radioactive waste and other radioactive material and the protective and mitigative measures to protect against potential large scale releases of fission products from malevolent actions.

* * * * *

12. In § 73.50, the introductory paragraph is revised to read as follows:

§ 73.50 Requirements for physical protection of licensed activities.

Each licensee who is not subject to §§ 73.51 or 73.53, but who possesses, uses, or stores formula quantities of strategic special nuclear material that are not readily separable from other radioactive material and which have total external radiation dose rates in excess of 100 rems per hour at a distance of 3 feet from any accessible surfaces without intervening shielding other than at nuclear reactor facility licensed pursuant to part 50 of this chapter, shall comply with the following:

* * * * *

13. In § 73.51, the heading is revised and paragraph (a) is revised to read as follows:

§ 73.51 Requirements for physical protection of stored spent nuclear fuel and high-level radioactive waste.

(a) *Applicability.* Notwithstanding the provisions of §§ 73.20, 73.50, or 73.67, the

physical protection requirements of this section apply to each licensee that stores spent nuclear fuel and high-level radioactive waste pursuant to paragraphs (a)(1) and (2) of this section. This includes spent nuclear fuel and high-level radioactive waste stored under a specific license issued pursuant to part 72 of this chapter:

(1) At an independent spent fuel storage installation (ISFSI) or

(2) At a monitored retrievable storage (MRS) installation.

14. Section 73.53 is added to read as follows:

§ 73.53 Requirements for physical protection of a geologic repository operations area.

(a) *Applicability*. Notwithstanding the provisions of §§ 73.20, 73.50, or 73.67, the physical protection requirements of this section apply to DOE for its activities at the geologic repository operations area (GROA) pursuant to a license issued under Part 60 or 63 of this chapter.

(b) *Submittal and implementation dates*. (1) DOE shall submit a Physical Security Plan, Training and Qualification Plan, and Safeguards Contingency Plan that delineate how the requirements of this section will be met. The security plans must be submitted no later than 180 days after the NRC issues a construction authorization for the GROA. The Commission-approved security plans must be implemented upon the Commission's issuance of a license to receive and possess source, special nuclear, or byproduct material at the GROA or by the date specified in a license condition.

(2) DOE is exempt from the requirements of this section after permanent closure of the GROA.

(c) *Performance objectives.*

(1) *General*. DOE shall establish, implement, and maintain an onsite physical protection program and security organization which will have as its objective to provide high assurance that activities involving radioactive waste are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

(2) *Radioactive waste containing strategic special nuclear material.* For formula quantities of strategic special nuclear material, DOE shall establish and maintain, or make arrangements for, a physical protection system designed to detect, assess, intercept, challenge, delay, and neutralize security-related events specified for theft or diversion of strategic special nuclear material and radiological sabotage as stated in § 73.1(a).

(3) *Radioactive waste not containing strategic special nuclear material.*

(i) For radioactive material that could result in a significant radiological sabotage event releasing radioactive materials in sufficient quantity such that any individual located at the controlled area boundary, or 400 meters (1300 ft), whichever is less, could receive a total effective dose equivalent equal to or greater than 0.25 Sv (25 rem), DOE shall establish and maintain, or make arrangements for, a physical protection system designed to detect, assess, intercept, challenge, delay and neutralize security-related events specified for radiological sabotage as stated in § 73.1(a)(1).

(ii) For radioactive material that could result in a moderate radiological sabotage event releasing radioactive materials in sufficient quantity such that any individual located at the controlled area boundary, or 400 meters (1300 ft), whichever is less, could receive a total effective dose equivalent equal to or greater than 0.05 Sv (5 rem) but less than 0.25 Sv (25 rem), DOE shall establish and maintain, or make arrangements for, a physical protection system designed to detect, assess, intercept, challenge, delay and neutralize, impede, or mitigate security-related events specified for radiological sabotage. DOE must protect against

an adversary force that is well-trained (including military training and skills) and contains dedicated individuals. The adversary force may include assistance from an inside knowledgeable individual participating in a passive role (e.g., provide information), an active role (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack), or both. The adversary force may be armed with suitable weapons, up to and including hand-held automatic weapons, equipped with silencers and having effective long range accuracy, and be equipped with hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying the facility, transporter, or container integrity or features of the safeguards system. The adversary force may use a four-wheel drive land vehicle used for transporting personnel and their hand-carried equipment or land vehicle bomb to the proximity of vital areas.

(iii) For all other radioactive material containing special nuclear material, DOE shall establish and maintain, or make arrangements for, a physical protection system designed to detect, assess, intercept, challenge, delay, and prevent the removal of special nuclear material from the protected area for security-related events specified for theft or diversion. DOE must protect against an adversary force that is well-trained (including military training and skills) and contains dedicated individuals. The adversary force may include assistance from an inside knowledgeable individual participating in a passive role (e.g., provide information), an active role (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack), or both. The adversary force may be armed with suitable weapons, up to and including hand-held automatic weapons, equipped with silencers and having effective long range accuracy, and be equipped with hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying the facility, transporter, or container integrity or features of the safeguards system. The adversary force may use a

four-wheel drive land vehicle used for transporting personnel and their hand-carried equipment or land vehicle bomb to the proximity of vital areas.

(iv) For other solidified radioactive material and Appendix P to part 110 - Category 1 and 2 Radioactive Material, DOE shall establish and maintain or make arrangements for a physical protection system designed to:

(A) Minimize the possibilities for unauthorized access to the radioactive material;

(B) Prevent or impede the removal of the radioactive material from the controlled area;

(C) Facilitate the location and prompt recovery of lost, stolen, or missing radioactive material; and

(D) Mitigate potential consequences of such security-related events.

(d) *General requirements*. DOE shall:

(1) Design and implement the physical protection program to satisfy the performance requirements of this section and ensure that no single act can disable the personnel, equipment, or systems necessary to prevent the theft of strategic special nuclear material and significant radiological sabotage. The physical protection program must include diverse and redundant equipment, systems, technology, programs, supporting processes, and implementing procedures;

(2) 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 (h) of this section and Appendix C to this part, through implementation of the DOE protective strategy. Except, the requirement for annual force-on-force exercises only applies to formula quantities of strategic special nuclear material and significant radiological sabotage consequence target sets;

(3) Establish, maintain, and follow an access authorization program for protected and vital areas that meets the requirements of § 73.56a and § 73.57;

(4) Develop, implement, and maintain an insider mitigation program. 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, DOE capability to prevent theft, diversion, and radiological sabotage of high-level radioactive waste; and

(5) 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.

(e) *Security plans.* DOE shall:

(1) Develop security plans that implement Commission requirements and that identify:

(i) How the physical protection program will prevent the theft or diversion and radiological sabotage of special nuclear and byproduct materials 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) Protect the security plans and other related safeguards information against unauthorized disclosure in accordance with the requirements of § 73.21 or Executive Order

12958, as appropriate.

(3) Establish, implement, and maintain 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. 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.

(4) Develop, implement, and maintain a process for DOE's written approval of implementing procedures and revisions to those procedures. The process shall ensure that implementing procedures and revisions to the procedures do not decrease the effectiveness of the security plans.

(5) Revise approved security plans as necessary to ensure the effective implementation of Commission regulations and DOE's protective strategy. Commission approval of revisions made pursuant to this paragraph is not required, provided that the revisions make no change that would decrease the effectiveness of any security plan prepared pursuant to this section. DOE shall submit a report containing a description of each change within six months after the change is made. DOE shall submit any change that decreases the effectiveness of any security plan for NRC approval pursuant to §§ 60.45 or 63.45 of this chapter.

(6) Establish, implement, and maintain a Commission-approved physical security plan that identifies how the performance objective and requirements set forth in this section will be implemented. The physical security plan must describe the facility location and layout; the security organization and structure; duties and responsibilities of personnel; and defense-in-depth implementation that describes components, equipment, and technology used. The physical security plan must include an assessment of radiological sabotage security events against the radiological dose criteria to determine the appropriate protective strategy for

identified target sets described in paragraph (h) of this section.

(7) Establish, maintain, and follow a Commission-approved training and qualification plan that identifies how the criteria set forth in Appendix B, “General Criteria for Security Personnel,’’ Section VII, to this part will be implemented. The training and qualification plan must describe the process by which armed and unarmed security personnel, watch persons, and other members of the security organization will be selected, trained, equipped, tested, qualified, and requalified to ensure that these individuals possess and maintain the knowledge, skills, and abilities required to carry out their assigned duties and responsibilities effectively.

(8) Establish, implement, and maintain a Commission-approved safeguards contingency plan that describes how the criteria set forth in Appendix C, ‘‘Licensee Safeguards Contingency Plans,’’ Section III, to this part will be implemented. The safeguards contingency plan must describe predetermined actions, plans, and strategies designed to respond to security related events.

(f) *Security organization.* DOE:

(1) 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. The security organization must include:

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

(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’s protective strategy.

(2) Shall 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, Section VII, to this part and the Commission-approved training and qualification plan.

(3) Shall not assign an individual to any position involving detection, assessment, or response to unauthorized activities unless that individual has satisfied the requirements of § 73.56a.

(4) Shall ensure that any written agreement with any contractor used to implement the onsite physical protection program must be retained as a record for the duration of the contract, and the agreement must clearly state the following conditions:

(i) DOE 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 DOE 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 § 73.56a;

(iv) An individual may not be assigned duties and responsibilities required to implement the approved security plans or DOE protective strategy unless that individual has been properly trained, equipped, and qualified to perform his or her assigned duties and responsibilities in accordance with Appendix B, Section VII, to this part and the Commission-approved training and qualification plan; and

(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.

(g) *Physical barriers.* DOE shall establish and maintain physical barriers in the controlled area to deter, delay, or prevent unauthorized access; facilitate the early detection of unauthorized activities; and control approach routes to the facility. Based upon DOE's protective strategy, analyses, and site conditions that affect the use and placement of physical barriers, DOE 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) DOE 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) DOE 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 standoff distance;

(ii) Be designed and constructed to protect against security-related events as specified by the Commission, commensurate to the required function of each barrier and in support of the DOE's protective strategy;

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

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

(4) *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, typically 6.1 m (20 feet) wide, to permit unobstructed observation and assessment of activities on either side of the protected area barrier; and

(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 any 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 DOE's capability to meet the requirements of paragraphs (g)(5)(i)(A) and (g)(5)(i)(B) must be located outside of the isolation zone.

(5) *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 are alarmed.

(iv) 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.

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

(6) *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 (h)(3) of this section.

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

(iii) Secondary power supply systems for intrusion detection and assessment equipment, nonportable communications equipment, and the alarm stations, 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 paragraph (t) of this section, and adjustments must be made to the site protective strategy, site procedures, and approved security plans, as necessary.

(v) DOE 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.

(7) *Vehicle barrier system.* DOE 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 objectives and requirements described in paragraphs (c) and (d) of this section, as appropriate;

(ii) Limit and control all vehicle approach routes;

(iii) Design and install a vehicle barrier system, to include passive and active barriers, at a standoff distance adequate to protect personnel, equipment, and systems against security-related events as specified by Commission requirements;

(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; and

(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.

(8) *Unattended openings*. 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.

(h) *Target sets*. DOE shall:

(1) 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) Consider the effects that cyber attacks may have upon individual equipment or elements of each target set or grouping.

(3) Explicitly identify in the approved security plans any target set equipment or elements that are not contained within a protected or vital area. Protective measures for such equipment or elements must be addressed by DOE's protective strategy in accordance with Appendix C to this part.

(4) Implement a program for the oversight of plant equipment and systems documented as part of DOE's protective strategy to ensure that changes to the configuration of the identified equipment and systems do not compromise DOE's capability to prevent or mitigate radiological sabotage.

(i) *Access control*. DOE shall establish an access control program with the features described in paragraphs (i)(1) through (i)(8) of this section.

(1) *General*. DOE 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 nonemergency 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 control equipment located at or outside of the protected area;

(vi) Isolate the individual responsible for the last 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; and

(vii) In response to a specific threat and security information, implement a two (2) 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, DOE shall implement measures to verify that the two-person rule has been met when a vital area is accessed.

(2) *Confirmation, verification, and search*. In accordance with the approved security plans and before granting unescorted access through an access control point, DOE shall:

(i) Confirm the identity of individuals;

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

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

(3) *Access control points*. Access control points must be:

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

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

(4) *Emergency conditions*. DOE shall:

(i) 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, 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; and

(C) The capability to prevent or mitigate radiological sabotage is maintained.

(iii) Ensure that restrictions for site access and egress during emergency conditions are coordinated with responses by emergency support organizations identified in the emergency plans required by § 60.21(c)(9) or § 63.161 of this chapter.

(5) *Vehicles.*

(i) DOE shall exercise control over all vehicles while inside the protected area and vital areas to ensure that 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 facility 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*. DOE 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) DOE 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. DOE 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; and

(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) DOE may permit escorted access to the protected area to individuals who do not

have unescorted access authorization in accordance with the requirements of § 73.56a of this part and part 26 of this chapter. DOE 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; and

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

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

(A) Nonemployee, no escort required;

(B) Areas to which access is authorized;

(C) The period for which access is authorized;

(D) The individual's employer; and

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

(8) *Escorts.* DOE shall ensure that all escorts are trained in accordance with Section VII

of Appendix B to this part, the approved training and qualification plan, and DOE 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.

(j) *Search programs.*

(1) At each designated access control point into the DOE-controlled area and protected areas, DOE 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 objectives and requirements of paragraphs (c) and (d) of this section, as appropriate.

(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 DOE, shall perform search activities or be assigned duties and responsibilities required to satisfy observation requirements for the search activities.

(2) DOE 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) DOE 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, DOE 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.

(k) *Detection and assessment systems.*

(1) DOE 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 (2) continuously staffed onsite alarm stations,

both of which must be protected in accordance with the requirements of paragraphs (g)(5)(iv), (g)(6)(iii), and (k)(8)(ii) of this section.

(3) DOE'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; and

(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 DOE protective strategy in the event that either alarm station is disabled.

(i) DOE 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 assistance, implement the protective strategy, provide command and control, or otherwise prevent radiological sabotage or mitigate consequences.

(ii) The alarm station functions in paragraph (k)(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) *Intrusion system capabilities*. DOE 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 provide the detection and assessment capabilities necessary to meet the requirements of paragraph (d) 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; and

(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 alarm stations must not be visible from the perimeter of the protected area.

(iii) DOE must 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) DOE shall assess and respond to all alarms and other indications of unauthorized activities in accordance with the approved security plans and implementing procedures.

(v) DOE'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) DOE 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) DOE 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, DOE shall initiate actions consistent with the approved security plans, DOE protective strategy, and implementing procedures.

(10) *Video technology.* DOE shall:

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

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

(ii) 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.* DOE shall:

(i) Ensure that all areas of the facility, to include appropriate portions of the DOE controlled area, are provided with illumination necessary to satisfy the requirements of this section;

(ii) Provide a minimum illumination level of 2.2 Lux (0.2 foot-candle) measured horizontally at ground level, in the isolation zones and all exterior areas within the protected area, or 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; and

(iii) 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.

(l) *Communication requirements.*

(1) DOE 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, watch-person, 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; and

(iii) A system for communication with on-duty operations personnel, escorts, local, State, and Federal law enforcement agencies, and all other personnel necessary to coordinate necessary responses.

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

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

(m) *Response requirements.*

(1) DOE shall:

(i) Establish and maintain, at all times, the minimum number of properly trained and equipped personnel required to intercept, challenge, delay, and/or neutralize security-related events as specified by the Commission for radiological sabotage and theft or diversion of special nuclear material.

(ii) 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, DOE's protective strategy, implementing procedures, and the site-specific conditions under which the firearms, ammunition, and equipment will be used.

(iii) 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) Ensure that all firearms, ammunition, and equipment required by the protective strategy and security plans are in sufficient supply, are in working condition, and are readily available for use in accordance with DOE protective strategy and predetermined timelines.

(v) 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 Section VII of Appendix B of this part

(2) DOE shall:

(i) 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 in accordance with the requirements of Part 1047 of this title, when the armed response person has a reasonable belief that the use of such force is necessary in self-defense or in the defense of others, or any other circumstances as authorized by applicable Federal law;

(ii) Provide an armed response consisting of a tactical response team, armed responders, and armed security officers to carry out response duties, within predetermined timelines;

(iii) Determine, subject to Commission approval, the minimum number of armed security

officers and armed responders necessary to protect against security events and document the numbers in the approved security plans;

(iv) Have armed responders available at all times inside the protected area. The armed responders may not be assigned any other duties or responsibilities that could interfere with assigned response duties. Armed security officers designated to strengthen response capabilities shall be onsite and available at all times to carry out assigned response duties; and

(v) Ensure that training and qualification requirements accurately reflect the duties and responsibilities to be performed.

(3) DOE 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 DOE in the approved security plans.

(4) DOE shall develop, maintain, and implement a written protective strategy in accordance with the requirements of this section and Appendix C to this part.

(5) DOE 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.

(6) Upon receipt of an alarm or other indication of threat, DOE 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, impede, or mitigate the threat in accordance with the requirements of Section III of Appendix C of this part, the Commission-approved safeguards contingency plan, and the DOE response strategy; and

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

(7) If offsite support is required, DOE shall document and maintain a pre-arranged plan with local, State, and/or Federal law enforcement agencies for assistance, in response to an actual theft of radioactive material.

(n) *Digital computer and communication networks.*

(1) *Cyber-security program*. DOE 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) DOE shall describe the cyber-security program requirements in the approved security plans.

(ii) DOE shall incorporate the cyber-security program into the 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*. DOE shall implement a cyber security assessment program to systematically assess and manage cyber risks.

(3) *Policies, requirements, and procedures.*

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

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

(4) *Incident response and recovery.*

(i) DOE 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 Section III of 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.* DOE 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.* DOE 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) DOE shall implement a cyber-security awareness and training program.

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

(o) *Security program reviews and audits*.

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

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

(ii) Within twelve (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 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) 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 from any response forces by local, State, and Federal law enforcement authorities, cyber-security programs, safety/security interface, and the testing, maintenance, and calibration program.

(3) DOE shall periodically review the approved security plans, the integrated response plan, DOE protective strategy, and licensee implementing procedures to evaluate their effectiveness and potential impact on facility and personnel safety.

(4) DOE 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) DOE shall conduct quarterly drills and annual exercises in accordance with Section III of Appendix C to this part and the DOE performance evaluation program. Except, the requirements for annual force-on-force exercises only apply to formula quantities of strategic special nuclear material and significant radiological sabotage consequence target sets.

(6) The results and recommendations of the 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 for DOE's management at least one level higher than that having responsibility for day-to-day facility operation.

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

(8) DOE 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 DOE protective strategy.

(9) Unless otherwise specified by the Commission, physical protection program reviews, audits, and assessments may be conducted up to thirty (30) days prior to, but no later than thirty (30) days after the scheduled date without adverse impact upon the next scheduled annual audit date.

(p) *Maintenance, testing, and calibration.*

(1) DOE 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 be 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 in the site's corrective action program. DOE shall protect this information as safeguards information, if applicable; and

(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 backup communication equipment, must be tested for operability at least once each day.

(6) Search equipment must be tested for operability at least once each day and tested for performance at least once during each seven-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 backup 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.

(q) *Compensatory measures.* DOE 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. 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. Compensatory measures must be implemented within specific timelines necessary to meet the requirements stated in paragraph (d) of this section and described in the approved security plans.

(r) *Suspension of safeguards measures.* DOE:

(1) May suspend implementation of affected requirements of this section under the following conditions:

(i) DOE 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 at a minimum by a designated senior site manager prior to taking this action; and

(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 designated senior site manager prior to taking this action.

(2) Must reimplement suspended security measures as soon as conditions permit; and

(3) Must report and document the suspension of safeguards measures in accordance with the provisions of § 73.71 of this part.

(s) *Records.* DOE 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. 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 DOE or a contractor.

(t) *Safety/security interface.* DOE 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 GROA safety:

(1) DOE shall assess and manage the potential for adverse affects on safety and security, including the site emergency plan, before implementing changes to GROA operations, 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).

(3) Where potential adverse interactions are identified, DOE 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.

(u) *Alternative measures.* (1) The Commission may authorize DOE to provide a measure for protection against radiological sabotage or theft or diversion other than one required by this section if DOE demonstrates that:

(i) The measure meets the same performance objectives and requirements as specified in paragraphs (c) and (d) of this section, as appropriate; and

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

(2) DOE shall submit each proposed alternative measure to the Commission for review and approval in accordance with § 60.45 or § 63.45, of this chapter, before implementation.

(3) DOE 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) In the case of alternative vehicle barrier systems required by paragraph (g)(7) of this section, DOE shall demonstrate that the alternative measure provides substantial protection against a vehicle bomb.

(v) *Additional requirements for Strategic Special Nuclear Material.* In addition to any

other requirements of this section, for formula quantities of strategic special nuclear material, DOE shall establish and maintain, or arrange for physical protection systems, subsystems, components, and procedures that provide the following additional performance capabilities for fixed site protection unless otherwise authorized by the Commission:

(1) *Security organization*.

(i) DOE's management system shall include written security procedures which detail the duties of the Tactical Response Team responsible for responding to security events involving strategic special nuclear material.

(ii) Tactical Response Team members shall also be trained and qualified in accordance with Section VII of Appendix B to this part. Upon the request of an authorized representative of the Commission, DOE shall demonstrate the ability of the physical security personnel, whether licensee or contractor employees, to carry out their assigned duties and responsibilities.

(iii) Within any given period of time, a member of the security organization may not be assigned to, or have direct operational control over, more than one of the redundant elements of a physical protection subsystem if such assignment or control could result in the loss of effectiveness of the subsystem.

(2) *Physical barrier subsystems.*

(i) In addition to the requirements in paragraph (g)(6) of this section, access to vital equipment, related to strategic special nuclear material, requires passage through at least three physical barriers.

(ii) Strategic special nuclear material must be stored or handled only in a material access area located within a protected area so that access to strategic special nuclear material requires passage through at least three physical barriers. (NOTE: A waste package or a cask is considered to be a barrier.)

(iii) The inner barrier of the protected area perimeter must be positioned and constructed to delay attempts at unauthorized exit from the protected area.

(iv) 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 or material access area within the protected area.

(3) *Access control subsystems and procedures.*

(i) In addition to the requirements of paragraph (i) of this section:

(A) Access to vital equipment, related to strategic special nuclear material and material access areas, shall include at least two individuals;

(B) Authorization for such individuals shall be indicated by the issuance of specially coded numbered badges indicating material access areas, and controlled access areas to which access is authorized; and

(C) No activities other than those which require access to strategic special nuclear material or to equipment used in the processing, use, or storage of strategic special nuclear material, or necessary maintenance, shall be permitted within a material access area.

(ii) DOE shall establish and follow written procedures that will permit access control personnel to identify those vehicles that are authorized and those materials that are not authorized entry to material access areas.

(iii) DOE shall control all points of personnel and vehicle access to material access areas, strategic special nuclear material vital areas, and strategic special nuclear material controlled access areas.

(A) At least two (2) armed guards, trained in accordance with the provisions contained in paragraph (d)(3) of this section and Section VII of Appendix B of this part, shall be posted at each material access area control point whenever in use.

(B) Identification and authorization of personnel and vehicles must be verified at the material access area control point.

(C) Prior to entry into a material access area, packages must be searched for firearms, explosives, and incendiary devices.

(4) *Search programs.*

(i) All vehicles, materials, and packages, including trash, wastes, tools, and equipment exiting from a material access area, must be searched for concealed strategic special nuclear material by a team of at least two individuals who are not authorized access to that material access area.

(ii) Each individual exiting a material access area shall undergo at least two (2) separate searches for concealed strategic special nuclear material. For individuals exiting an area that contains only alloyed or encapsulated strategic special nuclear material, the second search may be conducted in a random manner.

(iii) Before exiting from a material access area, containers of contaminated wastes must be drum scanned and tamper sealed by at least two (2) individuals, working and recording their findings as a team, who do not have access to material processing and storage areas.

(5) *Detection, surveillance, and alarm subsystems and procedures*. (i) All emergency exits in each material access and strategic special nuclear material vital area shall be locked to prevent entry from the outside and alarmed to provide local visible and audible alarm annunciation.

(ii) All unoccupied strategic special nuclear material vital areas and material access areas shall be locked and protected by an intrusion alarm subsystem which will alarm upon the entry of a person anywhere into the area, upon exit from the area, and upon movement of an individual within the area.

(iii) Vaults that contain strategic special nuclear material that has not been alloyed or encapsulated shall also be under the surveillance of closed circuit television that is monitored in both alarm stations. Additionally, means shall be employed which require that an individual other than an alarm station operator be present at, or have knowledge of access to, such unoccupied vaults or process areas.

(iv) Methods to observe individuals within material access areas to assure that strategic special nuclear material is not moved to unauthorized locations or in an unauthorized manner shall be provided and used on a continuing basis.

(v) Alarms occurring within unoccupied vaults and unoccupied material access areas containing unalloyed or unencapsulated strategic special nuclear material shall be assessed by at least two (2) security personnel using closed circuit television or other remote means.

(vi) Alarms occurring within unoccupied material access areas that contain only alloyed or encapsulated strategic special nuclear material shall be assessed by at least two (2) security personnel using closed circuit television or other remote means, or by at least two (2) security personnel who shall undergo a search before exiting the material access area.

(6) *Response requirements.* In addition to the armed response team, a Tactical Response Team consisting of a minimum of five (5) members must be available at the facility to fulfill assessment and response requirements.

(i) The size and availability of the Tactical Response Force must be determined on the basis of site-specific considerations that could affect the ability of the total onsite response force to neutralize security-related events consistent with DOE's protective strategy.

(ii) Each Tactical Response Team member shall be armed with a 9mm semiautomatic pistol. All but one member of the Tactical Response Team shall be additionally armed with a covered weapon as described in Section VII of Appendix B of this part.

(iii) The rationale for the total number, availability, and arming of Tactical Response Team personnel must be included in the security plans submitted to the Commission for approval.

(iv) DOE shall establish, maintain, and follow a Commission-approved safeguards contingency plan for responding to threats up to and including the design basis threats described in § 73.1(a), for theft or diversion and radiological sabotage related to formula quantities of strategic special nuclear material.

15. Section 73.56a is added to read as follows:

§ 73.56a Personnel access authorization requirements for a geologic repository operations area.

(a) *Applicability*. (1) DOE, as a licensee under Part 60 or Part 63 of this chapter, shall satisfy the requirements of this section upon receipt of Commission authorization to receive and possess source, special nuclear, or byproduct material at the geologic repository operations area. DOE shall submit the access authorization program for review and approval.

(2) DOE 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.

(3) 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 DOE relies upon those C/V authorization programs or program elements to meet the requirements of this section. In any case, only DOE shall grant or permit an individual to maintain unescorted access to the

protected and vital areas of a GROA.

(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 DOE grants unescorted access to protected and vital areas of a GROA;

(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 the operational safety, security, or emergency response capabilities;

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

(iv) DOE's or the C/V's reviewing official.

(2) At DOE's or the 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, paragraph (b)(2) of this section are trustworthy and reliable, such that they do not constitute an unreasonable risk to public health and safety or the common defense and security, including the potential to commit radiological sabotage, theft, or diversion.

(d) *Background investigation*. In order to grant unescorted access authorization to an individual, DOE and the 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*. DOE and the 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. DOE 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 DOE and C/Vs about the individual.

(i) The subject individual may withdraw his or her consent at any time. DOE or the C/V to whom the individual has applied for unescorted access authorization shall inform the individual that withdrawal of his or her consent will withdraw the individual's current application for access authorization under DOE's or the C/V's authorization program; and

(ii) If an individual withdraws his or her consent, DOE and the 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.

(iii) DOE and the 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; and

(C) 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 DOE's or the 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) DOE and the 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 DOE or a C/V.

(3) *Verification of true identity*. DOE 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, DOE 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, DOE 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*. DOE 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, DOE or the 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, DOE or the 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 DOE or the 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, DOE or the C/V shall document this refusal, inability, or unwillingness in DOE's, or the 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 DOE or the C/V to obtain information about the individual's character and reputation. If DOE or the C/V uses an alternate source because employment information is not forthcoming within 3 business days of the request, DOE or the 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 DOE, or any 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, DOE or a C/V who is subject to this section shall disclose whether the subject individual's unescorted access authorization was denied or terminated unfavorably.

DOE or the 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, DOE or the C/V may obtain information and documents by electronic means, including, but not limited to, telephone, facsimile, or email. DOE or the 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*. DOE and the 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*. DOE and the 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*. DOE's or the 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, DOE and the 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 DOE'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, theft, or diversion.

(1) DOE and the 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, paragraph (b)(2) of this section are subject to behavioral observation.

(2) The individuals specified in paragraph (b)(1) and, if applicable, paragraph (b)(2) of this section shall observe the behavior of other individuals. DOE and the 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 DOE or the C/V grants an initial unescorted access authorization, as defined in paragraph (h)(5) of this section, and must be current before DOE or the 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, theft or diversion. 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). DOE or the 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*. DOE and the 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*. DOE and the 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 DOE or the receiving 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, DOE and C/Vs may rely upon the information that other 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, DOE or the 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 or § 73.56 but whose unescorted access authorization has since been terminated under favorable conditions, DOE or the 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 DOE or the C/V grants unescorted access authorization to the individual. If potentially disqualifying information is disclosed or discovered about an individual, DOE and

C/V's shall take additional actions, as specified in the 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, DOE or the 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 DOE or the 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, DOE or the 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, DOE or the 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, DOE or the 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 DOE or the 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, DOE or the 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, DOE or the 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, DOE or the 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 DOE or the 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. DOE or the 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 DOE's or the C/V's control and DOE or the C/V is not aware of any potentially disqualifying information regarding the individual within the past 5 years, DOE or the 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, DOE or the C/V shall administratively withdraw the individual's unescorted access authorization until the employment history evaluation is completed.

(8) *Determination basis*. DOE's or the 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. DOE's or the 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*. DOE 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.

(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 paragraph (f)(2)(ii) of this section;

(iii) The individual complies with DOE's or the 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 DOE's Physical Security Plan; and

(v) DOE or the C/V determines that the individual continues to be trustworthy and reliable. This determination must be made as follows:

(A) DOE or the 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 Physical Security Plans, DOE or the 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 DOE or the 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*. DOE shall establish, implement, and maintain a list of individuals who are authorized to have unescorted access to specific 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 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*. DOE 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*. DOE 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*. DOE 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) DOE or the 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*. DOE and each 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. DOE may not

grant or permit the individual to maintain unescorted access authorization during the review process.

(m) *Protection of information*. DOE or each 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) DOE 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) DOE's or the 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 DOE and other 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, DOE or the 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) DOE's or a 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) DOE 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 DOE or a 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 DOE or the C/V to withhold evidence of criminal conduct from law enforcement officials.

(n) *Audits and corrective action*. DOE 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 DOE. DOE and each 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) DOE and each 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. DOE 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 DOE by C/V personnel who are off site or are not under the direct daily supervision or observation of DOE'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) DOE's 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) DOE's contracts with C/Vs, and a C/V's contracts with subcontractors, must also require that DOE 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 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. DOE or the 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) DOE may jointly conduct audits, or may accept audits of C/Vs that were conducted by other licensees and applicants who are subject to § 73.56, 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 or § 73.56, if the audit addresses the services obtained from the subcontractor by each of the sharing licensees, applicants, and C/Vs.

(i) DOE 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 DOE or the 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) DOE and each C/V shall maintain a copy of the shared audit, including findings, recommendations, and corrective actions.

(o) *Records*. DOE and each 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 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) DOE and each C/V who is subject to this section shall retain the following records for at least 5 years after DOE or the 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) DOE and each 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) DOE 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) DOE 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 DOE or the C/V, or until the completion of any legal proceedings relating to the actions of such authorization program personnel, whichever is later.

(6) If DOE or a C/V administratively withdraws an individual's unescorted access authorization under the requirements of this section, DOE or the 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, DOE or the 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.

16. In § 73.57, the heading is revised, paragraph (a)(4) is added; paragraphs (b)(2)(iii) and (b)(2)(iv) are redseignated as (b)(2)(iv) and (b)(2)(v); a new paragraph (b)(2)(iii) is

added; and paragraphs (b)(1), (b)(4), (b)(4)(i), (b)(5), (b)(8), (c)(1), (d)(1), (d)(3)(ii), (f)(2), and (f)(5) are revised to read as follows:

§ 73.57 Requirements for criminal history checks of individuals granted unescorted access to a nuclear power facility, the protected area of a geologic repository operations area, or access to Safeguards Information by power reactor licensees.

(a) ***

(4) DOE, as a licensee under Part 60 or Part 63 of this chapter, shall comply with the requirements of this section upon receipt of Commission authorization to receive and possess source, special nuclear, or byproduct material at the geologic repository operations area.

(b) ***

(1) Except those listed in paragraph (b)(2) of this section, each licensee subject to the provisions of this section shall fingerprint each individual who is permitted unescorted access to the nuclear power facility or access to Safeguards Information or unescorted access to the protected area of a GROA. Individuals who have unescorted access authorization on April 1, 1987 will retain such access pending licensee receipt of the results of the criminal history check on the individual's fingerprints, so long as the cards were submitted by September 28, 1987. The licensee will then review and use the information received from the Federal Bureau of Investigation (FBI), and based on the provisions contained in this rule, determine either to continue to grant or to deny further unescorted access to the facility or Safeguards Information for that individual. Individuals who do not have unescorted access or access to Safeguards Information after April 1, 1987 shall be fingerprinted by the licensee and the results of the criminal history records check shall be used prior to making a determination for granting unescorted access to the nuclear power facility, the protected area of a GROA, or access to

Safeguards Information.

(2) ***

(iii) For unescorted access to the protected area of a GROA, NRC employees and NRC contractors on official agency business; individuals responding to a site emergency in accordance with the provisions of § 73.53(s); a representative of the International Atomic Energy Agency (IAEA) engaged in activities associated with the U.S./IAEA Safeguards Agreement at designated facilities who has been certified by the NRC; law enforcement personnel acting in an official capacity; State or local government employees who have had equivalent reviews of FBI criminal history data; and individuals employed at a facility who possess "Q" or "L" clearances or possess another active government granted security clearance, i.e., Top Secret, Secret, or Confidential;

* * * * *

(4) Fingerprinting is not required if the utility is reinstating the unescorted access to the nuclear power facility, unescorted access to the protected area of a GROA, or access to Safeguards Information granted an individual if:

(i) The individual returns to the same nuclear power utility or GROA that granted access and such access has not been interrupted for a continuous period of more than 365 days; and

* * * * *

(5) Fingerprints need not be taken, in the discretion of the licensee, if an individual who is an employee of a licensee, contractor, manufacturer, or supplier has been granted unescorted access to a nuclear power facility, unescorted access to the protected area of a GROA, or to Safeguards Information by another licensee, based in part on a criminal history records check under this section. The criminal history check file may be transferred to the gaining licensee in accordance with the provisions of paragraph (f)(3) of this section.

* * * * *

(8) A licensee shall use the information obtained as part of a criminal history records check solely for the purpose of determining an individual's suitability for unescorted access to the nuclear power facility, unescorted access to the protected area of a GROA, or access to Safeguards Information.

(c) ***

(1) A licensee may not base a final determination to deny an individual unescorted access to the nuclear power facility, unescorted access to the protected area of a GROA, or access to Safeguards Information solely on the basis of information received from the FBI involving:

* * * * *

(d) ***

(1) For the purpose of complying with this section, licensees shall, using an appropriate method listed in § 73.4, submit to the NRC's Division of Facilities and Security, Mail Stop T-6E46, one completed, legible standard fingerprint card (Form FD-258, ORIMDNRCOOOZ) or, where practicable, other fingerprint record for each individual requiring unescorted access to the nuclear power facility, unescorted access to the protected area of a GROA, or access to Safeguards Information, to the Director of the NRC's Division of Facilities and Security, marked for the attention of the Division's Criminal History Check Section. Copies of these forms may be obtained by writing the Office of Information Services, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, by calling (301) 415-7232, or by e-mail to *forms@nrc.gov*. Guidance on what alternative formats might be practicable is referenced in § 73.4. The licensee shall establish procedures to ensure that the quality of the fingerprints taken results in minimizing the rejection rate of fingerprint cards due to illegible or incomplete cards.

* * * * *

(3) ***

(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 nuclear plant licensee or GROA licensee, and an administrative processing fee assessed by the NRC. The NRC processing fee covers administrative costs associated with NRC handling of licensee fingerprint submissions. The Commission publishes the amount of the fingerprint check application fee on the NRC public Web site. (To Find the current fee amount, go to the Electronic Submittals page at *http://www.nrc.gov/site-help/eie.html* and select the link for the Criminal History Program.) The Commission will directly notify licensees who are subject to this regulation of any fee changes.

* * * * *

(f) ***

(2) The licensee may not disclose the record or personal information collected and maintained to persons other than the subject individual, his/her representative, or to those who have a need to have access to the information in performing assigned duties in the process of granting or denying unescorted access to the nuclear power facility, unescorted access to the protected area of a GROA, or access to Safeguards Information. No individual authorized to have access to the information may re-disseminate the information to any other individual who does not have a need to know.

* * * * *

(5) The licensee shall retain all fingerprint and criminal history records received from the FBI, or a copy if the individual's file has been transferred, on an individual (including data indicating no record) for 1 year after termination or denial of unescorted access to the nuclear

power facility or unescorted access to the protected area of a GROA, or access to Safeguards Information.

17. In § 73.70, the introductory paragraph is revised and paragraph (c)(1) is added to read as follows:

§ 73.70 Records.

Each record required by this part must be legible throughout the retention period specified by each Commission regulation. The record may be the original or a reproduced copy or a microform provided that the copy or microform is authenticated by authorized personnel and that the microform is capable of producing a clear copy throughout the required retention period. The record may also be stored in electronic media with the capability for producing legible, accurate, and complete records during the required retention period. Records, such as letters, drawings, and specifications, must include all pertinent information such as stamps, initials, and signatures. The licensee shall maintain adequate safeguards against tampering with and loss of records. Each licensee subject to the provisions of §§ 73.20, 73.25, 73.26, 73.27, 73.45, 73.46, 73.53, 73.55, or 73.60 shall keep the following records:

* * * * *

(c) ***

(1) A register of visitors, vendors, and other individuals not employed by DOE pursuant to § 73.53(i)(7)(i)(C). DOE shall retain this register as a record, available for inspection, for three (3) years after the last entry is made in the register.

* * * * *

18. Section 73.71a is added to read as follows:

§ 73.71a Reporting of safeguards events for a GROA.

(a) DOE, as a licensee subject to the provisions of § 73.53, shall notify the NRC Operations Center 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 V of Appendix G to this part.

(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 (d) of this section, as applicable.

(b) DOE shall notify the NRC Operations Center within 1 hour of discovery of the safeguards events described in paragraph VI of Appendix G to this part. Notifications must be made according to paragraph (d) of this section, as applicable.

(c) DOE 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 VII of Appendix G to this part. Notifications must be made according to paragraph (d) of this section, as applicable.

(d) DOE shall make the telephonic notifications required by paragraphs (a), (b), and (c) 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, DOE 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 paragraph (a), (b), and (c) of this section, as applicable.

(2) Telephonic reports required by this section shall be made by DOE using secure telecommunications equipment approved for the transmission of safeguards information and classified information.

(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, and any immediate actions to stabilize the facility. 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 paragraph (b) 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 (c) of this section, the licensee is not required to maintain an open, continuous communication channel with the NRC Operations Center.

(e) DOE shall maintain a current safeguards event log.

(1) DOE shall record the safeguards events described in paragraph VI of Appendix G to this part within 24 hours of discovery.

(2) DOE 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.

(f) DOE shall make written reports as follows:.

(1) DOE shall make an initial telephonic notification under paragraphs (a) and (b) of this section and shall also submit a written report to the NRC within a 60-day period by an appropriate method listed in § 73.4.

(2) DOE is not required to submit a written report following a telephonic notification made under paragraph (c) of this section.

(3) DOE shall submit to the Commission written reports that are of a quality that will permit legible reproduction and processing.

(4) DOE shall prepare the written report in letter format.

(5) In addition to the addressees specified in § 73.4, DOE shall also provide one copy of the written report addressed to the Director, Office of Nuclear Security and Incident Response.

(6) The report must include sufficient information for NRC analysis and evaluation.

(7) 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 (d) of this section and also submitted in a revised written report (with the revisions indicated) as required under paragraph (f)(5) of this section.

(8) Errors discovered in a written report must be corrected in a revised report with revisions indicated.

(9) The revised report must replace the previous report; the update must be complete and not be limited to only supplementary or revised information.

(10) DOE 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.

19. In Appendix B to Part 73, a new Section VII is added to the table of contents, the introductory text is revised by adding a new paragraph between the first and second undesignated paragraphs, and Section VII is added to read as follows:

APPENDIX B TO PART 73—GENERAL CRITERIA FOR SECURITY PERSONNEL

* * * * *

Table of contents

Introduction

* * * * *

Insofar as DOE is subject to the requirements of § 73.53 of this part, DOE shall comply only with the requirements in Section VII of this appendix. All other licensees, applicants, or certificate holders shall comply only with Sections I through V of this appendix .

* * * * *

VII. Geologic Repository Operations Area Training and Qualification Plan.

A. General requirements and introduction.

1. DOE shall ensure that all individuals who are assigned duties and responsibilities required to prevent high-level radioactive waste theft or diversion and radiological sabotage and who implement the Commission-approved security plans, DOE response strategy, and implementing procedures, meet minimum training and qualification requirements to ensure that 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, DOE 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. DOE 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, DOE protective strategy, and the DOE 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. DOE 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. DOE 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; and

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

b. An unarmed individual assigned to the security organization may not have any felony

convictions that reflect on the individual’s reliability.

c. 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, DOE 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, DOE 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) DOE 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 DOE 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 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 than 40 decibels at any one frequency.

(2) A hearing aid is acceptable provided that 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, and the capability to implement instructions and assigned tasks, and shall 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 B.3.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. DOE 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) DOE 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, DOE 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 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 Commission-approved training and qualification plan.

b. Each individual who is assigned duties and responsibilities identified in the Commission-approved security plans, DOE 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; and

(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 DOE 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, DOE protective strategy, and implementing procedures, before the individual is assigned the duty or responsibility.

b. In addition to meeting the requirement stated in paragraph C.2.a. of this section, 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, DOE 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; and

(12) Command and control duties.

3. Tactical response team drills and exercises.

a. DOE shall demonstrate response capabilities through a performance evaluation program as described in Appendix C to this part.

b. DOE shall conduct drills and exercises in accordance with Commission-approved security plans, DOE 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, DOE 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, DOE 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 to 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 recertification exceed three (3) years.

c. Annual firearms familiarization. DOE 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) Drawing and pointing 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; and

(15) Weapon familiarization.

e. DOE shall ensure that each armed member of the security organization is instructed on the use of deadly force as authorized by applicable Federal or 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 requalified at least annually.

2. Alternate weapons qualification. Upon written request by DOE, the Commission may authorize DOE to provide firearms qualification programs other than those listed in this appendix if DOE demonstrates that the alternative firearm qualification program satisfies Commission requirements. Written requests must provide information regarding the proposed firearms qualification programs and describe how the proposed alternative satisfies Commission requirements.

3. Tactical weapons qualification. The DOE 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, DOE protective strategy, and implementing procedures. DOE-developed qualification and requalification courses for each firearm must describe the performance criteria needed, including the site-specific conditions (such as lighting, elevation, fields-of-fire) under which assigned personnel shall be required to carryout their assigned duties.

4. Firearms qualification courses. DOE 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 semiautomatic 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 semiautomatic 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 in paragraph F.5. 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 requalified 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.

DOE shall provide armed personnel with weapons that are capable of performing the function stated in the Commission-approved security plans, DOE protective strategy, and implementing procedures.

2. Personal equipment.

a. DOE 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, DOE protective strategy, and implementing procedures.

b. DOE 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; and

(5) Two-way portable radios (handi-talkie) 2 channels minimum, 1 operating and 1 emergency.

c. Based upon the DOE protective strategy and the specific duties and responsibilities assigned to each individual, DOE 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; and

(7) Tear gas or other non-lethal gas.

3. Maintenance.

Firearms maintenance program. DOE 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; and

(6) Armorer certification.

H. Records.

1. DOE shall retain all reports, records, or other documentation required by this appendix in accordance with the requirements of § 73.53(s).

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

3. DOE 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.

DOE shall review the Commission-approved training and qualification plan in accordance with the requirements of § 73.55(o).

J. Definitions.

Terms defined in parts 60, 63, and 73 of this chapter have the same meaning when used in this appendix.

20. 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 "Content of the Plan," and a new Section III 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 § 73.53, shall comply with the requirements of Section I of this appendix.

* * * * *

Section III: Geologic repository operations area 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 personnel to facilitate the initiation and completion of predetermined and exercised responses to threat scenarios, up to and including the design basis threat described in § 73.1(a), for radioactive waste containing strategic special nuclear material.

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) DOE 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) Records, audits and reviews.

(12) Implementing procedures.

(c) Background.

(1) Consistent with the design basis threat specified in § 73.1(a), DOE shall identify and describe the perceived dangers, threats, and incidents against which the safeguards contingency plan is designed to protect up to and including the design basis threat as specified in § 73.1(a).

(2) DOE shall describe the general goals and operational concepts underlying implementation of the approved safeguards contingency plan to include, but not be 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 shall provide at all times the capability to detect, assess, deter, 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. DOE shall include preplanned strategies for the GROA of potential events, including those that may result in the loss of large areas of the facility due to explosions or fire;

(iv) How the onsite response effort is organized and coordinated to ensure that the capability to prevent high-level radioactive waste theft and 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 restore the facility, 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 facility due to explosions or fires; and

(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) DOE 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) DOE 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; and

(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) DOE planning base.

DOE 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. The safeguards contingency plan must include a site description, to include maps and drawings, of the physical structures and their locations.

(i) 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.

(ii) 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.

(3) Safeguards systems hardware. The safeguards contingency plan must contain a description of the physical security and material accounting system hardware that influence how DOE 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 the number of personnel, types of weapons, and estimated response timelines.

(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 Federal laws, State laws, local ordinances, and policies and practices that govern DOE response to incidents and must include, but not be limited to, the following:

(i) Use of deadly force;

(ii) Recall of off-duty employees;

(iii) Site jurisdictional boundaries; and

(iv) Use of enhanced weapons, if applicable.

(6) Administrative and logistical considerations. The safeguards contingency plan must contain a description of DOE practices which influence how DOE responds to a threat to include, but not be 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) DOE 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) DOE shall identify and discuss potential areas of conflict between site plans in the integrated response plan required by Section III(b)(8) of this appendix.

(4) DOE shall address safety/security interface issues in accordance with the requirements of § 73.53(t) to ensure that 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) DOE 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, DOE 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) DOE 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) The DOE 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) DOE 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) DOE shall identify the personnel, equipment, and resources necessary to perform the actions required to prevent sabotage in response to postulated events.

(3) DOE shall ensure that predetermined actions can be completed under the postulated conditions.

(4) DOE 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) DOE 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) DOE 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 high-level radioactive waste theft or diversion and radiological sabotage through the coordinated implementation of specific actions and strategies required to intercept, challenge, delay, and neutralize, impede, or mitigate security-related threats;

(ii) Describe and consider site-specific conditions, to include but not be 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 high-level radioactive waste theft or diversion or sabotage;

(iii) Identify predetermined actions and timelines for the deployment of armed personnel;

(iv) Provide bullet resisting protected positions with appropriate fields of fire; and

(v) Limit exposure of security personnel to possible attack.

(3) DOE shall provide a command and control structure, to include response by offsite 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) DOE shall document, maintain, and implement an Integrated Response Plan which must identify, describe, and coordinate actions to be taken by DOE 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 restore the facility 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 facility 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; and

(v) Include specific procedures, guidance, and strategies describing cyber incident response and recovery.

(3) DOE shall:

(i) Reconfirm on an annual basis, liaison with local, State, and Federal law enforcement agencies, established in accordance with § 73.53(m)(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 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) DOE shall implement a “Threat warning system” which identifies specific graduated protective measures and actions to be taken to increase preparedness against a heightened or imminent threat of attack.

(2) DOE 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, DOE shall implement the specific protective measures assigned to the threat level indicated by the Commission representative.

(l) Performance Evaluation Program.

(1) DOE shall document and maintain a Performance Evaluation Program that describes how the DOE will demonstrate and assess the effectiveness of the onsite physical protection program to prevent significant radiological sabotage events 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 DOE’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 DOE 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) DOE shall document each performance evaluation to include, but not be 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) DOE 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, DOE protective strategy, and implementing procedures.

(vi) DOE 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, DOE 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 that reflect the capabilities of armed personnel to neutralize a target through the use of firearms during drills and exercises; and

(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 DOE protective strategy participates in at least one (1) drill on a quarterly basis and one (1) force-on-force exercise on an annual basis, as appropriate;

(ii) The mock adversary force replicates, as closely as possible, adversary characteristics and capabilities in the design basis threat described in § 73.1(a) of this part, and is capable of exploiting and challenging the DOE 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; and

(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) DOE shall develop and document multiple scenarios for use in conducting quarterly drills and annual force-on-force exercises.

(ii) DOE 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 be limited to, equipment, implementing procedures, and personnel.

(iv) DOE 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) DOE shall review and audit the Commission-approved safeguards contingency plan in accordance with the requirements § 73.53(o).

(2) DOE 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) DOE shall retain all reports, records, or other documentation required by this appendix in accordance with the requirements of § 73.53(s).

(n) Implementing procedures.

(1) DOE 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) DOE 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.

21. In Appendix G to Part 73, a paragraph is added after the introductory paragraph and paragraphs V, VI, VII and VIII are added to read as follows:

APPENDIX G TO PART 73—REPORTABLE SAFEGUARDS EVENTS

* * * * *

Under the provisions of § 73.71a DOE, as a licensee subject to the provisions of § 73.53, shall report or record, as appropriate, the following safeguards events under paragraphs V, VI, VII, and VIII of this appendix. DOE shall make such reports to the Commission under the provisions of 73.71a.

* * * * *

V. *Events at a GROA 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 DOE's physical security plan, safeguards contingency plan, or defensive strategy based on actual or imminent threat.

(b) DOE 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.

VI. *Events at a GROA 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 the GROA facility if it possesses strategic special nuclear material; or

(3) Interruption of normal operation of the GROA 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 DOE 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 DOE 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 DOE is required by Commission regulations to control access.

VII. *Events at a GROA 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 not be 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 facility, or challenges to security

systems (e.g., failure to stop for security checkpoints or possible tests of security response and security screening equipment.

(2) Any security-related incident involving suspicious aircraft overflight activity. Commercial or military aircraft activity considered routine by DOE is not required to be reported.

(3) Any incident resulting in the notification of local, state or national law enforcement, or law enforcement response to the site not included in paragraphs V or VI of this appendix;

(b) The unauthorized use of or tampering with the components or controls, including the security system.

(c) Follow-up communications regarding events reported under paragraph VII of this appendix will be completed through the NRC threat assessment process via the NRC Operations Center.

VIII. *Events at a GROA 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 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.

PART 74 - MATERIAL CONTROL AND ACCOUNTING OF SPECIAL NUCLEAR MATERIAL

22. The authority citation for Part 74 continues to read as follows:

AUTHORITY: Secs. 53, 57, 161, 182, 183, 68 Stat. 930, 932, 948, 953, 954, as amended, sec. 234, 83 Stat. 444, as amended, sec.1701, 106 Stat. 2951, 2952, 2953, (42 U.S.C.2073, 2077, 2201, 2232, 2233, 2282, 2297f); 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).

23. In § 74.1, paragraph (b) is revised to read as follows:

§ 74.1 Purpose.

* * * * *

(b) The general conditions and procedures for the submittal of a license application for the activities covered in this part are detailed in §§ 60.21, 63.21, or 70.22 of this chapter.

24. In § 74.2, paragraph (b) is revised to read as follows:

§ 74.2 Scope.

* * * * *

(b) In addition, specific control and accounting requirements are included in subparts C, D, E, and F of this part for certain licensees who:

(1) Possess and use formula quantities of strategic special nuclear material;

(2) Possess and use special nuclear material of moderate strategic significance;

(3) Possess and use special nuclear material of low strategic significance;

(4) Possess uranium source material and equipment capable of producing enriched uranium; or

(5) Possess and use waste containing special nuclear material at a GROA.

* * * * *

25. In § 74.4, definitions for *accounting*, *custodian*, *high-level radioactive waste*, *item control area*, *item control program*, and *material balance area* are added in alphabetical order to read as follows:

§ 74.4 Definitions.

* * * * *

Accounting means the records (e.g., ledgers, journals, source documents, etc.) pertaining to the determination of, and current record maintenance of, special nuclear material quantities associated with receipts, shipments, measured discards, transfers into and between material balance areas and/or item control areas, and total material on current inventory.

* * * * *

Custodian means a designated individual who is responsible for the control and movement of all special nuclear material within a specified control area, and maintaining records relative to all special nuclear material transferred into or out of the area and that is currently located within the control area. Control areas are usually designated as material balance areas or item control areas. From the standpoint of appropriate safeguards practice, a single individual should not be a custodian of more than one control area.

* * * * *

High-level radioactive waste or *HLW* means:

(1) The highly radioactive material resulting from the reprocessing of spent nuclear fuel, including liquid waste produced directly in reprocessing and any solid material derived from such liquid waste that contains fission products in sufficient concentrations;

(2) Irradiated reactor fuel; and

(3) Other highly radioactive material that the Commission, consistent with existing law, determines by rule requires permanent isolation.

* * * * *

Item control area (ICA) means an identifiable physical area for the storage and control of special nuclear material items. Control of items moving into or out of an ICA is by item identity and assigned special nuclear material quantity.

Item control program means a system that tracks (i.e., records) the creation, identity, location, and disposition of all special nuclear material items of certain predetermined categories. In addition, item control programs usually provide a periodic verification of item existence and location for static items.

* * * * *

Material balance area (MBA) means an identifiable physical area for the physical and administrative control of special nuclear material such that the quantity of nuclear material being moved into or out of the MBA is a measurement-based assigned value for element and isotope.

* * * * *

26. In § 74.13, paragraph (a) is revised to read as follows:

§ 74.13 Material Status Reports.

(a) Each licensee, including nuclear reactor licensees as defined in §§ 50.21 and 50.22

of this chapter, authorized to possess at any one time and location special nuclear material in a quantity totaling more than 350 grams of contained uranium-235, uranium-233, or plutonium, or any combination thereof, shall complete and submit, in computer-readable format, Material Balance Reports concerning special nuclear material that the licensee has received, produced, possessed, transferred, consumed, disposed of, or lost. This prescribed computer-readable report replaces the DOE/NRC Form 742 which has been previously submitted in paper form. The Physical Inventory Listing Report must be submitted with each Material Balance Report. This prescribed computer-readable report replaces the DOE/NRC Form 742C which has been previously submitted in paper form. Each licensee shall prepare and submit the reports described in this paragraph in accordance with instructions (NUREG/BR-0007 and NMMSS Report D-24 "Personal Computer Data Input for NRC Licensees"). Copies of these instructions may be obtained from the U.S. Nuclear Regulatory Commission, Office of Nuclear Material Safety and Safeguards, Washington, DC 20555-0001. Each licensee subject to the requirements of § 74.51 shall compile a report as of March 31 and September 30 of each year and file it within 30 days after the end of the period covered by the report. All other licensees subject to this requirement shall submit a report within 60 calendar days of the beginning of the physical inventory required by §§ 74.19(c), 74.31(c)(5), 74.33(c)(4), 74.43(c)(6), or 74.73(i)(1). The Commission may permit a licensee to submit the reports at other times for good cause.

* * * * *

27. In § 74.17, a new paragraph (d) is added to read as follows:

§ 74.17 Special nuclear material physical inventory summary report.

* * * * *

(d) DOE shall submit a completed Special Nuclear Material Physical Inventory Summary Report on NRC Form 327 not later than 60 calendar days from the start of each physical inventory required by § 74.73(i). DOE shall report the physical inventory results by facility and total facility to the Director, Office of Nuclear Material Safety and Safeguards, U.S. Nuclear Regulatory Commission.

28. In § 74.19, paragraphs (a) and (c) are revised to read as follows:

§ 74.19 Recordkeeping.

(a) Licensees subject to the recordkeeping requirements of §§ 74.31, 74.33, 74.43, 74.59, or 74.73 are exempt from the requirements of paragraphs (a)(1) through (a)(4) of this section. Otherwise:

* * * * *

(c) Other than licensees subject to §§ 74.31, 74.33, 74.41, 74.51, or 74.71, each licensee who is authorized to possess special nuclear material, at any one time and site location, in a quantity greater than 350 grams of contained uranium-235, uranium-233, or plutonium, or any combination thereof, shall conduct a physical inventory of all special nuclear material in its possession under license at intervals not to exceed 12 months. The results of these physical inventories need not be reported to the Commission, but the licensee shall retain the records associated with each physical inventory until the Commission terminates the license that authorized the possession of special nuclear material.

* * * * *

29. Subpart F is redesignated as Subpart G and a new Subpart F is added to read

as follows:

Subpart F - Geologic Repository Operations Area

§ 74.71 Nuclear material control and accounting for a geologic repository operations area.

(a) *General performance objectives*. DOE shall establish, implement, and maintain a Commission-approved material control and accounting (MC&A) program that will achieve the following performance objectives:

(1) Maintain accurate, current, and reliable information on, and confirm the quantities and locations of special nuclear material (SNM) in radioactive waste in DOE's possession at the GROA;

(2) Detect, respond to, and resolve any anomalies indicating a possible loss of SNM, including potential theft or diversion;

(3) Permit rapid determination of whether an actual loss of a significant quantity of SNM has occurred;

(4) Generate and provide, as requested, information to aid in the investigation and recovery of missing SNM in the event of an actual loss, theft, or other misuse; and

(5) Control access to MC&A information that might assist adversaries in possible attempts to carry out a theft or diversion, or to help target radioactive waste for radiological sabotage.

(b) *System capabilities*. To achieve the general performance objectives in § 74.71(a), the MC&A program must include the capabilities and features described in § 74.73.

(c) *Submittal and implementation dates*. DOE shall submit an MC&A plan describing how the performance objectives of § 74.71(a) will be achieved, and how the system capabilities

required by § 74.71(b) will be met. The MC&A plan must be submitted no later than 180 days after the NRC issues a construction authorization for the GROA. The Commission-approved MC&A plan must be implemented upon the Commission's issuance of a license to operate the GROA or by the date specified in a license condition.

§ 74.73 Internal controls, inventory, and records.

(a) *General*. DOE shall establish and maintain the internal control, inventory, and recordkeeping capabilities required in paragraphs (b) through (k) of this section.

(b) *Management structure*. DOE shall:

(1) Establish, document, and maintain a management structure that assures clear overall responsibility for MC&A functions, independence of MC&A functions from operations responsibilities, and separation of key responsibilities; and

(2) Provide for the adequate review, approval, and use of written procedures that are identified in the approved MC&A plan as being critical to the effectiveness of the described program.

(c) *Personnel qualification and training*. DOE shall assure that personnel, who work in key positions where mistakes could degrade the effectiveness of the MC&A system, are trained to maintain a high level of safeguards awareness and are qualified to perform their duties and/or responsibilities.

(d) *Independent assessments*. DOE shall perform and document independent reviews and assessments of the total MC&A program, at intervals not to exceed 24 months, that assess the performance of the program, review its effectiveness, and document management's action on prior assessment recommendations and identified deficiencies.

(e) *Item control program*. DOE shall establish, document, implement, and maintain an item control program that:

(1) Provides current knowledge of all SNM items with respect to unique identity, element and isotope content, and location from receipt to underground emplacement to retrieval (if necessary);

(2) Assures that the integrity of items is maintained by the tamper-safing of containers; placement in a controlled access area that provides protection at least equivalent to tamper-safing; or sealing such that the unauthorized removal of SNM would be readily apparent.

(3) Maintains and follows procedures for tamper-safing of containers, which include control of access to and distribution of unused seals and records showing the date and time of seal application;

(4) Stipulates the use of the 2-person rule for sealing operations, for affixing tamper-indicating devices, for any handling of bare fuel assemblies, for taking and/or verifying physical inventories or for transfers of SNM.

(5) Designates item control areas (ICA) and ICA custodians.

(f) *Anomaly, detection, and response program*. DOE shall establish, implement, and maintain a program that:

(1) Detects and responds to anomalies indicating a potential loss or misuse of SNM, including the possible theft or diversion of SNM by an internal threat using collusion, stealth, and deceit. The overall design of the detection and response program must include an analysis of conceivable ways and means through which clandestine attempts of theft, diversion, or other misuse might occur; and

(2) Incorporates checks and balances that are sufficient to thwart an attempt to divert SNM and to detect falsification of data and reports that could conceal the theft or diversion of SNM by:

(i) A single individual, including an employee in any position; and

(ii) Collusion between individuals, one or more of whom have authorized access to SNM.

(g) *Quality assurance capabilities*. DOE shall establish, document, implement, and maintain a program to reasonably assure the validity of assigned SNM quantities, including a measurement system and a measurement control program that:

(1) Maintains a level of effectiveness sufficient to satisfy the capabilities required for detection, response, and accounting. To achieve this objective, DOE shall perform engineering analyses and evaluations of the design, installation, preoperational tests, calibration, and operation of all measurement systems to be used for MC&A systems; and

(2) Assures the validity of the assigned SNM content for receipts on a shipment basis by:

(i) Checking unique identification, integrity and intactness of shipments;

(ii) Coordinating with originators regarding the technical bases and assignment of SNM values, the loading of canisters/shipping casks, and tamper-safing/sealing procedures for shipping SNM to the GROA;

(iii) Investigating and resolving any discrepancies that may arise from validity checks on receipts or from off-normal circumstances; and

(iv) Using, as needed, weighing and/or nondestructive assay measurements for verifying SNM content in the resolution of anomalies or other off-normal circumstances from receipt to emplacement.

(h) *Information aid*. To meet the general performance objective in § 74.71(a)(4) DOE shall provide to the NRC and/or other appropriate government agencies information deemed necessary for conducting an investigation of actual (or highly suspected) events pertaining to missing SNM and information relevant to the recovery of missing SNM from theft, diversion, or other loss.

(i) *Inventory*. DOE shall:

(1) Except as required by part 75 of this chapter, perform a facility-wide physical inventory of all possessed SNM to close material balances on an annual basis;

(2) Provide written instructions for conducting physical inventories that detail assignments, responsibilities, preparation for and performance of an inventory, and assure that all items are listed, and no item is listed more than once;

(3) Designate material balance areas (MBA) and MC&A data-base administrators. MBAs shall be designated for taking physical inventories of specified underground and surface operations; and

(4) Within 60 days after the start of each physical inventory required by paragraph (i)(1) of this section:

(i) Reconcile and adjust the book record, as appropriate, to the results of the physical inventory;

(ii) Investigate and resolve, or report, by an appropriate method listed in § 74.6 to the Director, Office of Nuclear Material Safety and Safeguards, any unresolved inventory difference or discrepancy.

(j) *Measures for formula quantities of strategic SNM*. If DOE receives formula quantities of strategic special nuclear materials at the GROA that are in a form other than as irradiated reactor fuel or high-level radioactive waste, such strategic SNM shall be controlled and accounted for in a manner that meets the following additional program measures:

(1) Item monitoring features as specified in § 74.55;

(2) Alarm resolution as specified in § 74.57;

(3) Quality assurance and accounting capabilities, as appropriate, as specified in § 74.59;

(4) Establishment of controlled areas for strategic special nuclear material; and

(5) Conduct of a semiannual physical inventory of all strategic special nuclear material.

(k) *Recordkeeping*. (1) DOE shall:

(i) Establish records that will demonstrate that the performance objectives of § 74.71(a) and the system capability and feature requirements of § 74.73 have been met, and maintain these records in duplicate in an auditable form, available for inspection, and retain these records until the Commission terminates the GROA license;

(ii) Retain material control and accounting procedures until the Commission terminates the GROA license and retain any superseded portion of the procedure for 3 years after the portion is superseded;

(iii) Maintain adequate safeguards against tampering with and loss of records;

(iv) Satisfy the requirements of § 60.71 or § 63.71 of this chapter, for records on the receipt, handling, and disposition of radioactive waste at the GROA.

(2) Records that must be maintained pursuant to this part may be the original or a reproduced copy or a microform if the reproduced copy or microform is duly authenticated by authorized personnel, and the microform is capable of producing a clear and legible copy after storage for the period specified by Commission regulations. The record may also be stored in

electronic media with the capability for producing legible, accurate, and complete records during the required retention period. Records such as letters, drawings, or specifications must include all pertinent information such as stamps, initials, and signatures.

Dated at Rockville, Maryland, this_____ day of_____, 2007.

For the Nuclear Regulatory Commission.

_____
Annette Vietti-Cook,
Secretary of the Commission.