[7590-01-P]

NUCLEAR REGULATORY COMMISSION

10 CFR Parts 26, 50, 52, 72, 73, and 95

[PRM-26-4; PRM-26-7; PRM-26-8; NRC-2012-0079; and NRC-2025-1303]

RIN 3150-AL53

Modernizing Security Requirements

AGENCY: Nuclear Regulatory Commission.

ACTION: Proposed rule and draft guidance; request for comment.

SUMMARY: The U.S. Nuclear Regulatory Commission (NRC) is proposing to revise its regulations to modernize security and fitness-for-duty requirements to enhance efficiency, consistent with Executive Order 14300, “Ordering the Reform of the Nuclear Regulatory Commission.” The proposed revisions are intended to reduce regulatory burden, where appropriate, while continuing to provide reasonable assurance that safety and security will be adequately maintained at NRC-licensed facilities.

DATES: Comments must be submitted electronically using https://www.regulations.gov by 11:59 p.m. eastern time on **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

ADDRESSES: Submit your comments, identified by Docket ID NRC-2025-1303, at https://www.regulations.gov. If your material cannot be submitted using https://www.regulations.gov, call or email the individuals listed in the FOR FURTHER INFORMATION CONTACT section of this document for alternate instructions.

Do not include any personally identifiable information (such as name, address, or other contact information) or confidential business information that you do not want publicly disclosed. All comments are public records; they are publicly displayed exactly as received and will not be deleted, modified, or redacted. Comments may be submitted anonymously.

Follow the search instructions on https://www.regulations.gov to view public comments.

You can read a plain language description of this proposed rule at https://www.regulations.gov/docket/NRC-2025-1303. For additional direction on obtaining information and submitting comments, see “Obtaining Information and Submitting Comments” in the SUPPLEMENTARY INFORMATION section of this document.

FOR FURTHER INFORMATION CONTACT: Nicole Fields, Office of Nuclear Material Safety and Safeguards, telephone: 630-829-9570, email: Nicole.Fields@nrc.gov and Shyrl Coker, Office of Nuclear Reactor Regulation, telephone: 301-287-3603, email: Shyrl.Coker@nrc.gov. Both are staff of the U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

SUPPLEMENTARY INFORMATION:

EXECUTIVE SUMMARY:

A. Need for the Regulatory Action

The U.S. Nuclear Regulatory Commission (NRC) is proposing to revise its regulations to modernize security and fitness-for-duty requirements to enhance efficiency, consistent with Executive Order 14300, “Ordering the Reform of the Nuclear Regulatory Commission.”

B. Major Provisions

Major provisions of this proposed rule, supported by accompanying draft guidance, include the following:

- *Fitness for Duty Programs*. The NRC is proposing effectiveness and efficiency improvements to the drug and alcohol testing requirements based on lessons learned from implementing title 10 of the *Code of Federal Regulations* (10 CFR) part 26, “Fitness for Duty Programs,” to align with select changes made by other Federal agency testing programs, and to address several petitions for rulemaking (PRMs). Changes include enabling the collection and drug testing of oral fluid specimens for all conditions

for testing, a risk-informed reduction in the annual random testing rate for most licensee employees, enhancing blind performance testing requirements with additional program flexibilities and targeted sampling reductions, updating the refresher training interval, and eliminating the requirement for licensees to conduct annual audits of U.S. Department of Health and Human Services certified laboratories. The NRC also is proposing to extend the duration of applicability for the optional subpart K to 10 CFR part 26 fitness-for-duty programs for reactor construction, and to enable licensees and other entities to escort construction workers instead of subjecting those workers to a subpart K program. Under the fatigue management program requirements, the NRC is proposing to add a new exception from the work-hour controls for sequestration events, specifying alternative work hour controls and requirements that licensees may meet during such events. The NRC is also proposing to eliminate the annual reporting of fatigue management performance information to the NRC. These changes would reduce unnecessary regulatory burden.

- *Security Requirements for Independent Spent Fuel Storage Installations*. The proposed rule would revise security requirements for independent spent fuel storage installations (ISFSIs) to improve clarity and consistency between the requirements for general license ISFSIs and specific license ISFSIs. Major provisions would allow standalone ISFSIs located outside a power reactor's protected area to implement security programs appropriate for their risk profile. The rule would streamline the process for updating ISFSI security plans and reduce the frequency of required submissions to the NRC. These changes would be responsive to stakeholder feedback and Commission direction, reducing licensee burden and facilitating efficient transitions to decommissioning.

- *Physical Security Requirements.* The NRC is proposing to modernize and streamline physical security requirements for nuclear power reactors and materials by shifting from prescriptive rules to performance-based, risk-informed criteria. The amendments would provide increased flexibility for implementing security measures and

allow for the use of technology-inclusive approaches and alternatives tailored to diverse reactor designs. The proposal addresses access authorization, cybersecurity, safeguards information handling, event notifications, and training, and resolves industry concerns from recent rulemakings. In revising performance objectives, the changes would support innovation, reduce unnecessary regulatory burden, and maintain protection against credible threats.

- *Facility Security Clearance and Safeguarding of National Security Information and Restricted Data*. The NRC is proposing to revise 10 CFR part 95, “Facility Security Clearance and Safeguarding of National Security Information and Restricted Data,” to remove requirements that are duplicative and to ensure alignment with 32 CFR part 117, “National Industrial Security Program Operating Manual (NISPOM).” These changes would provide references to the applicable provisions of 32 CFR part 117 for implementation of the National Industrial Security Program.

C. Costs and Benefits

The NRC prepared a draft regulatory analysis to determine the expected quantitative costs and benefits of this proposed rule and associated draft guidance as well as qualitative factors to be considered in the NRC’s rulemaking decision. The conclusion from the analysis is that this proposed rule and associated draft guidance would result in net cost savings to the industry and the NRC, over the next 30 years, ranging from $561 million using a 7 percent discount rate to $1.01 billion using a 3 percent discount rate. For the industry, the net cost savings are estimated at $557 million (7 percent discount rate) and $1.01 billion (3 percent discount rate). For the NRC, the net cost savings are estimated at $3.4 million (7 percent discount rate) and $6.7 million (3 percent discount rate). On an annualized basis, the net cost savings to the industry and the NRC would be about $45.2 million per year at a 7 percent discount rate and $51.8 million per year at a 3 percent discount rate.

The draft regulatory analysis also considers qualitative factors, such as regulatory efficiency. These benefits would result from clarifications, administrative

changes, and streamlining of processes (such as notifications), along with aligning requirements with existing Federal regulations instead of maintaining separate but similar NRC requirements.

For more information, please see the draft regulatory analysis (available in the NRC's Agencywide Documents Access and Management System (ADAMS) Accession No. ML26113A051).

TABLE OF CONTENTS:

I. Obtaining Information and Submitting Comments

A. Obtaining Information

Please refer to Docket ID NRC-2025-1303 when contacting the NRC about the availability of information for this action. You may obtain publicly available information related to this action by any of the following methods:

- **Federal Rulemaking Website:** Go to https://www.regulations.gov and search for Docket ID NRC-2025-1303.
- **NRC's Agencywide Documents Access and Management System (ADAMS):** You may obtain publicly available documents online in the ADAMS Public Documents collection at https://www.nrc.gov/reading-rm/adams.html. To begin the search, select "Begin ADAMS Public Search." For problems with ADAMS, please contact the NRC's Public Document Room (PDR) reference staff at 1-800-397-4209, at 301-415-4737, or by email to PDR.Resource@nrc.gov. For the convenience of the reader, instructions about obtaining materials referenced in this document are provided in the "Availability of Documents" section.
- **NRC's PDR:** The PDR, where you may examine and order copies of publicly available documents, is open by appointment. To make an appointment to visit the PDR, please send an email to PDR.Resource@nrc.gov or call 1-800-397-4209 or 301-415-4737, between 8 a.m. and 4 p.m. eastern time, Monday through Friday, except Federal holidays.
- **Public Meeting:** The NRC will conduct a public meeting to describe the proposed amendments and answer questions from the public on the proposed rule. The NRC will publish a notice of the location, time, and agenda of the meeting on the NRC's public meeting website within 10 calendar days of the meeting. Stakeholders should monitor the NRC's public meeting website for information about the public meeting at: https://www.nrc.gov/public-involve/public-meetings/index.cfm.

B. Submitting Comments

Comments must be submitted electronically using https://www.regulations.gov no later than 11:59 p.m. eastern time on **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**. Please include Docket ID NRC-2025-1303 in your comment submission.

The NRC cautions you not to include identifying or contact information that you do not want to be publicly disclosed in your comment submission. The NRC will post all comment submissions at https://www.regulations.gov as well as enter the comment submissions into ADAMS. The NRC does not routinely edit comment submissions to remove identifying or contact information.

If you are requesting or aggregating comments from other persons for submission to the NRC, then you should inform those persons not to include identifying or contact information that they do not want to be publicly disclosed in their comment submission. Your request should state that the NRC does not routinely edit comment submissions to remove such information before making the comment submissions available to the public or entering the comment into ADAMS.

II. Executive Order 14300: Ordering the Reform of the Nuclear Regulatory Commission

On May 23, 2025, President Donald J. Trump signed Executive Order (E.O.) 14300, “Ordering the Reform of the Nuclear Regulatory Commission.” Section 5, “Reforming and Modernizing the NRC’s Regulations,” requires the NRC to undertake a review and wholesale revision of its regulations and guidance documents as guided by the policies set forth in section 2 of the E.O. This rulemaking addresses section 5(g), which directs the NRC to “[r]evise the Reactor Oversight Process and reactor security rules and requirements to reduce unnecessary burdens and be responsive to credible risks.”

III. Background

Over the decades, the NRC has developed a comprehensive regulatory framework to ensure that licensee programs at nuclear facilities provide reasonable assurance that public health and safety is adequately protected and are in accord with the common defense and security. This proposed rule seeks to modernize the NRC's regulatory framework for licensee security programs—reducing regulatory burden, where appropriate, while continuing to provide reasonable assurance of adequate safety and security. The principal regulations relevant to this proposed rule are set forth in 10 CFR parts 26; 72, "Licensing Requirements for the Independent Storage of Spent Nuclear Fuel, High-Level Radioactive Waste, and Reactor-Related Greater Than Class C Waste"; 73, "Physical Protection of Plants and Materials"; and 95.

The regulations in 10 CFR part 26 govern fitness-for-duty (FFD) programs, including drug and alcohol testing and fatigue management, for personnel at nuclear power plants and certain other NRC-licensed facilities. The requirements are designed, in part, to provide reasonable assurance that individuals are trustworthy, reliable, and not under the influence of any substances, legal or illegal, or mentally or physically impaired from any cause that could adversely affect their ability to safely and competently perform their duties.

The regulations in 10 CFR part 72 set forth requirements for the licensing and operation of ISFSIs. These facilities are used to safely store spent nuclear fuel and certain other radioactive materials, both at power reactor sites and away from reactor sites. Part 72 includes both safety and security provisions, with physical protection requirements that vary depending on whether the ISFSI is operated under a general license or specific license.

The regulations in 10 CFR part 73 address the physical protection of plants and materials. Part 73 contains detailed requirements for physical security programs, access authorization, cybersecurity, and the protection of safeguards information. These requirements apply to commercial nuclear power reactors, fuel cycle facilities, and other

licensees that possess special nuclear material (SNM). The regulation is structured to protect against the design basis threats of radiological sabotage and theft or diversion of SNM, and includes requirements for security organization, training, response strategies, and contingency planning.

The regulations in 10 CFR part 95 establish requirements for facility security clearances and the safeguarding of national security information and restricted data. These requirements are intended to ensure that NRC licensees and certificate holders who require access to classified information maintain appropriate security measures in accordance with the National Industrial Security Program.

The NRC recognizes the need to modernize and streamline its security and FFD regulations to reduce unnecessary regulatory burden, promote regulatory clarity, provide appropriate program flexibility, and support the deployment of innovative technologies, while also continuing to provide reasonable assurance that safety and security will be adequately maintained. This proposed rule aligns with national policy directives to facilitate the expansion of United States nuclear energy capacity, as articulated in recent Executive Orders and statutory mandates.

In addition to E.O. 14300, other recent E.O.s related to the expansion of United States nuclear energy capacity include E.O. 14156, “Declaring a National Energy Emergency” (90 FR 8433; January 29, 2025), which stressed the need for a reliable, diversified, and affordable supply of energy, and E.O. 14154, “Unleashing American Energy” (90 FR 8353; January 29, 2025), which stated that it is in the national interest to “unleash America’s affordable and reliable energy and national resources.”

Recent statutory mandates related to nuclear energy capacity include the Nuclear Energy Innovation and Modernization Act (Pub. L. 115-439, 132 Stat. 5572) (NEIMA) and the Accelerating Deployment of Versatile, Advanced Nuclear for Clean Energy Act of 2024 (Pub. L. 118-67, 138 Stat. 1448) (ADVANCE Act). In response to NEIMA, the NRC recently issued a final rule establishing 10 CFR part 53, “Risk-Informed, Technology-Inclusive Regulatory Framework for Commercial Nuclear Power

Plants," which sets forth a regulatory framework for licensing and regulating advanced reactors (91 FR 15696; March 30, 2026). Part 53 is designed to accommodate a wide range of reactor technologies and business models, providing performance-based requirements that enable the use of modern safety and security approaches. As discussed in Section IV of this document, proposed changes as a part of this proposed rule would apply to licensees and applicants under 10 CFR parts 50, "Domestic Licensing of Production and Utilization Facilities"; 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants"; and 53. The proposed amendments are intended to provide enhanced regulatory flexibility for both current and future licensees, streamline administrative processes, and ensure that NRC requirements remain effective, efficient, and responsive to credible risks.

The NRC prepared an unofficial redline strikeout version of the proposed changes to regulatory text that is intended to help the reader identify the changes. The unofficial redline strikeout version of the proposed rule is publicly available and is listed in the "Availability of Documents" section. Comments on the rule text should refer to this proposed rule and not the unofficial redline strikeout version.

IV. Discussion

The discussion is organized by subject area because of the wide-ranging set of issues covered by this proposed rule. The proposed rule also includes minor editorial corrections.

A. Fitness for Duty Programs (Part 26)

The proposed rule would incorporate effectiveness and efficiency improvements into the NRC's FFD program requirements for drug and alcohol testing and fatigue management since the NRC's extensive amendments of part 26 in 2008 (73 FR 17176; March 31, 2008). These proposed effectiveness and efficiency changes would reduce unnecessary regulatory burden on licensees and other entities and address section 5(g) of E.O. 14300. This proposed rule focuses on three areas: 1) incorporating lessons

learned from implementing part 26 since 2008; 2) aligning part 26 with select updates made to the U.S. Department of Health and Human Services (HHS) Mandatory Guidelines for Federal Workplace Drug Testing Programs (HHS Guidelines) and the U.S. Department of Transportation (DOT) drug testing requirements in 49 CFR part 40, "Procedures for Transportation Workplace Drug and Alcohol Testing Programs"; and 3) addressing three PRMs.[1]

Proposed changes to the drug and alcohol testing program requirements include the following: expanding the option to collect and drug test oral fluid specimens for all conditions for testing in § 26.31(c); implementing a risk-informed reduction to the annual random testing rate in § 26.31(d)(2)(vii) that applies to most licensee employees (i.e., those that do not perform critical safety- or security-related functions); extending the duration of applicability for the optional FFD program for reactor construction under subpart K to 10 CFR Part 26, "FFD Program for Construction"; enabling licensees and other entities to escort construction workers performing activities under § 26.4(f), as an alternative to those workers being subject to an FFD program; enhancing the § 26.168 blind performance testing requirements to reduce unnecessary burden; eliminating annual audits of HHS-certified laboratories performed by licensees and other entities; updating the FFD program refresher training interval; and removing unused regulations (specifically, subpart F, "Licensee Testing Facilities"). Proposed changes to the fatigue management program requirements include alternative requirements that licensees can meet during a sequestration event and the elimination of the requirement to annually report fatigue management information to the NRC.

From 2010 through 2012, the NRC also received three PRMs (docketed by the NRC as PRM-26-4, PRM-26-7, and PRM-26-8), which the NRC determined to be appropriate for consideration in the rulemaking process; all three of the PRMs are being

---

[1] The PRMs (PRM-26-4, PRM-26-7, and PRM-26-8) are discussed in this section and in Section IV.A.(i)(s), "SAE credential—State-licensed or -certified marriage and family therapists," and Section IV.A.(i)(t), "SAE credential—Certified Addiction Specialist by the American Academy of Health Care Providers in Addictive Medicine," of this document.

considered as part of this rulemaking. To address PRM-26-4, “California Association of Marriage and Family Therapists” (75 FR 51958; August 24, 2010), the NRC is proposing to add State-licensed or State-certified marriage and family therapists to the list of acceptable credentials in § 26.187(b) that qualify individuals to serve as substance abuse experts (SAEs). The NRC also considered the issues identified for rulemaking in PRM-26-7, “Certification of Substance Abuse Experts” (76 FR 61625; October 5, 2011), related to Certified Addiction Specialists. The NRC is not proposing to add the petitioner’s requested Certified Addiction Specialist that has been certified by the American Academy of Health Care Providers in the Addictive Disorders to the list of acceptable credentials to serve as an SAE under § 26.187(b), and accordingly would deny PRM-26-7.

Finally, the NRC considered the issues identified for rulemaking in PRM-26-8, “Additional Synthetic Drug Testing” (78 FR 22209; April 15, 2013). The NRC determined that the 2022 part 26 final rule (87 FR 71422; November 22, 2022), in part, addressed the issues raised in this petition by expanding the drug testing panel to include additional semi-synthetic opioids (hydrocodone, hydromorphone, oxycodone, oxymorphone), methylenedioxy-methamphetamine (MDMA), and methylenedioxyamphetamine (MDA). Under § 26.31(d)(1)(i), licensees and other entities also have the ability to consult with local law enforcement, hospitals, and drug counseling services to determine if other drugs with abuse potential are being used in the geographic locale of facilities, and to expand the drug testing panels to include any controlled substance that is listed on Schedules I through V of section 202 of the Controlled Substances Act. In addition, under § 26.77(b), a licensee or other entity must take immediate action to prevent any individual from performing covered duties if they appear impaired, which provides reasonable assurance that impairment from any cause (including the use of both scheduled and unscheduled substances) can be addressed. Accordingly, the NRC is not proposing changes related to PRM-26-8 and would deny this petition.

HHS and DOT have also updated their drug testing program requirements since the 2008 and 2022 amendments to part 26. On October 12, 2023, HHS published final revisions to the HHS Guidelines for the testing of drugs in urine and oral fluid specimens (88 FR 70768 and 88 FR 70814, respectively). DOT published two final rules amending its drug and alcohol testing programs in 49 CFR part 40. One updated DOT's urine drug testing requirements (82 FR 52229; November 13, 2017), and the other enabled oral fluid drug testing (88 FR 27596; May 2, 2023). The HHS Guidelines govern Federal employee workplace drug testing programs at more than 100 Federal agencies and Federal agency drug testing programs (e.g., DOT) that test civilians in safety- and security-sensitive positions similar to personnel tested under the NRC's FFD program in part 26. The NRC has historically relied on the HHS Guidelines to establish the technical requirements for the collection and testing of specimens for drugs and the review of test results. The NRC also relies on the DOT's drug and alcohol testing regulations in 49 CFR part 40 in certain situations for which HHS does not have guidelines; for example, the HHS Guidelines do not cover testing for alcohol or evaluating and returning individuals to covered duties following a positive drug or alcohol test result. The DOT-regulated entities also test millions of individuals each year, which provides valuable lessons learned from implementing a testing program covering a much larger worker population than exists in the U.S. nuclear industry. This proposed rule would incorporate select updates to the HHS Guidelines and DOT drug testing requirements into part 26.

(i) Drug and Alcohol Testing

(a) Program implementation milestone

The proposed rule includes a risk-informed change that would extend the implementation milestone for when a licensee or other entity must transition from the optional subpart K to an FFD program that meets all of the requirements of part 26, except subparts K and M, "Fitness for Duty Programs for Facilities Licensed under 10 CFR Part 53." The milestone would change from the receipt of special nuclear material in the form of fuel assemblies to before initial fuel load into the reactor.

The NRC has reassessed the risks presented during the construction of nuclear power reactors and has determined that implementation of § 26.3(a) and (c) and § 26.4(e)(1) is not commensurate with current risk insights. Section 26.3(a) currently requires, in part, that licensees authorized to operate a nuclear power reactor under part 50 and holders of a combined license (COL) under part 52 after the Commission has made the finding under § 52.103(g) shall implement the FFD program under the requirements of part 26, except for subparts K and M, before the receipt of SNM in the form of fuel assemblies. Under § 26.3(c), licensees and other entities constructing a nuclear power plant must implement their FFD program no later than receipt of SNM in the form of fuel assemblies. The risk associated with unirradiated fuel, however, does not increase when the fuel arrives onsite, because its engineered safety features, storage, and configuration have not changed since the fuel was in transit. For transit and receipt onsite, the same physical protection requirements (i.e., § 73.67, “Licensee fixed site and in-transit requirements for the physical protection of special nuclear material of moderate and low strategic significance”) are applied to protect the fuel. Safety and security risks associated with unirradiated nuclear fuel begin to increase once the process of loading fuel into its operating configuration begins. The operational milestone “before initial fuel load into the reactor” therefore corresponds more closely to the start of NRC-licensed activities that could result in consequences adverse to public health and safety or the common defense and security than does the current milestone of receipt of nuclear fuel onsite. Further, this proposed milestone change is based on recent operating experience from implementing subpart K FFD programs at power reactor construction sites. Specifically, the NRC issued an exemption to the licensee for Vogtle Electric Generating Plant Units 3 and 4 to delay implementing FFD programs, except those that applied for construction, until initial fuel load (86 FR 73809; December 28, 2021).

(b) Specimen testing options

The proposed rule would expand the option to collect and drug test oral fluid specimens for all conditions of testing specified under § 26.31(c). This proposed change would provide an effective method to thwart attempts to subvert the drug testing process because all oral fluid specimens would be collected under direct observation. Each year, approximately 25 to 30 percent of the drug testing violations under part 26 are identified subversion attempts. In most cases, a donor attempts to provide a specimen that did not come from their body (e.g., synthetic urine). This action is possible because a donor typically provides a urine specimen inside a privacy enclosure. However, oral fluid testing is conducted in a manner that is directly observable without the privacy enclosure associated with collecting a urine sample, and therefore precludes potential subversion attempts that can be visually identified.

Currently, under § 26.83(b), licensees and other entities have the option to collect and drug test an oral fluid specimen instead of a urine specimen only when a directly observed collection is required (i.e., when information suggests a donor may be attempting to subvert a urine drug test). Expanding the collection and drug testing of oral fluid specimens has the potential to significantly improve the deterrent capabilities of the drug testing process, which would improve public health and safety and common defense and security. This proposed rule would also reduce the financial and administrative burdens associated with actions taken in response to subversion attempts that licensees and other entities would no longer encounter.

(c) Blind performance testing submissions

Blind performance test samples (BPTSs) are formulated to verify the accuracy and reliability of each drug and validity test performed by the HHS-certified laboratory that a licensee or other entity uses to perform testing under contract. In each calendar quarter, BPTSs must be submitted to the laboratory for each drug or drug metabolite that must be tested in donor specimens and for each validity test performed to identify subversion attempts. A licensee or other entity must prepare BPTSs to appear as donor

specimens to the laboratory, and BPTSs must be submitted along with donor specimens throughout the calendar quarter to evaluate laboratory performance.

Each year, operating experience demonstrates that the BPTS program identifies unsatisfactory performance at HHS-certified laboratories. Given the consolidated use of testing laboratories by industry, an identified performance issue at one laboratory generally impacts numerous licensee and other entity FFD programs. Identified performance issues, for example, have pertained to false negative test results because of laboratory certified scientists failing to adhere to laboratory testing procedures, weaknesses in laboratory standard operating procedures, improperly formulated reagents used in testing, and testing equipment maintenance issues.

The proposed rule would incorporate three effectiveness and efficiency improvements for blind performance testing programs based on industry practice and lessons learned. These improvements would reduce unnecessary regulatory burden for licensees and other entities.

1. *Testing during initial 90 days*

The proposed rule would eliminate the increased number of BPTSs that must be submitted in the initial 90 days of a licensee or other entity initiating a contract with a new HHS-certified laboratory. Under the existing requirements in § 26.168(a), in this initial 90-day period, a minimum of 30 BPTSs must be submitted for testing, whereas in each subsequent calendar quarter, a minimum of 10 BPTSs must be submitted for testing. The increased number of BPTS submissions in the initial 90 days of testing is unnecessary. The NRC has found that the post-initial 90-day period BPTS submission number of 10 BPTSs per calendar quarter is sufficient to identify unsatisfactory laboratory performance. The blind testing program already requires that, if unsatisfactory performance is identified (e.g., false negative test result for a BPTS formulated to test positive for marijuana), a licensee or other entity must take immediate action to investigate and implement corrective actions under §§ 26.719(c) and 26.167(f). Eliminating the increased number of BPTSs in the initial 90 days of testing would also

reduce an unnecessary financial and administrative burden on a licensee or other entity considering changing to another HHS-certified testing laboratory.

2. *Fleetwide BPTS submissions*

The proposed rule would revise § 26.168(a) to clarify how a licensee or other entity is to determine how many BPTSs it must submit for testing in each calendar quarter, after the initial 90-day period, to the HHS-certified laboratory that it maintains under contract to perform testing. The current BPTS submission requirements require a minimum of 10 BPTSs to be submitted per quarter, or 1 percent of the donor specimens up to a maximum of 100 BPTSs, whichever is greater. Generally, § 26.168(a) has been applied at the facility level (e.g., a location with one or more nuclear power reactors), whereby the minimum BPTS submission requirement almost always applies. However, § 26.168(a) could also be interpreted to apply at the fleet level. That is, a utility could calculate the number of BPTSs to submit to its HHS-certified laboratory based on the total number of donor specimens submitted for testing from all its facilities each quarter. This application would result in a reduction in the number of BPTS submissions per quarter compared to treating each of the utility's facilities independently under § 26.168(a). Either application would adequately maintain safety and security because the testing capabilities of the laboratory used by the licensee would be effectively challenged throughout each testing quarter. Current industry practice demonstrates that a small number of HHS-certified laboratories are used by a large number of part 26-regulated entities (regardless of whether the number of BPTS submittals is calculated at the facility or the fleet level), which ensures that the HHS-certified laboratories undergo adequate testing, focusing on those program elements unique to the NRC's FFD framework.

3. *Quarterly drug testing submissions*

The NRC is proposing to eliminate the BPTS submission requirements in § 26.168(b)(1) and (2) that require a licensee or other entity to submit at least two BPTSs positive for marijuana in each quarter and to replace the BPTS positive for PCP with an additional BPTS positive for cocaine in at least two quarters per year. These

prescriptive requirements are unnecessarily restrictive to effectively challenge testing performed at HHS-certified laboratories (e.g., changing drug use trends may warrant a licensee to adjust which substances it submits to the laboratory, once it meets the minimum required in a quarter). The NRC is also proposing clarifications to § 26.168(d) for false negative challenge BPTSs and § 26.168(f) for negative BPTSs, which require a minimum of 10 percent of BPTSs submitted each quarter to be false negative challenge BPTSs and negative BPTSs, respectively. To conform with § 26.168(e) for validity testing BPTSs, the NRC is proposing to include a statement in each requirement to clarify that either a minimum of one BPTS, or 10 percent of BPTSs submitted each quarter, whichever is greater, must be submitted per quarter.

(d) Escorting construction workers

The proposed rule would amend part 26 to permit licensees and other entities to escort construction workers performing activities covered under § 26.4(f) instead of requiring these workers to be subject to an FFD program. This proposed change is based on recent operating experience from implementing subpart K FFD programs at the Vogtle Electric Generating Plant Units 3 and 4. Specifically, the NRC issued an exemption to the Vogtle licensee to permit the escorting of construction workers (84 FR 27364; June 12, 2019). To permit escorting, the proposed rule would amend § 26.5, “Definitions,” to define the word “Escort”; § 26.4(e) to include a new requirement that individuals that serve as an escort must be subject to an FFD program that meets all part 26 requirements, except subparts I, “Managing Fatigue,” K, and M; § 26.4(f) to state that individuals who are escorted and constructing or directing the construction of safety- or security-related structures, systems, and components (SSCs) need not be subject to the licensee’s FFD program; § 26.27(c)(5) and § 26.606(b)(7) to require the licensee or other entity to establish, implement, and maintain written procedures for escorting; and § 26.403(a) and (b) to require the licensee or other entity implementing a subpart K FFD program to establish, carry out, and maintain a procedure for escorts and those individuals under escort. These proposed changes would improve regulatory flexibility

and potentially reduce costs by enabling licensees and other entities the opportunity to better plan and carry out construction activities with individuals who may be onsite for only short periods of time.

(e) Fitness for duty program refresher training

The proposed rule would revise § 26.29(c)(2) to change the FFD program refresher training interval from a nominal 12-month frequency to a nominal 24-month frequency. This proposed change would align with the refresher training interval that would apply to future part 53 licensees and other entities that implement § 26.608(b) of subpart M. The proposed rule would maintain the requirement in existing §§ 26.29(c)(2) and 26.608(b) for refresher training to be performed more frequently than the specified interval if the need is indicated, such as when an individual fails to properly implement FFD program procedures, or because of the severity of problems discovered through licensee-performed FFD program audits. This proposed change would reduce unnecessary regulatory burden by providing licensees and other entities with more flexibility on when to perform FFD program refresher training.

(f) Random testing rates for licensee employees

The proposed rule would revise § 26.31(d)(2)(vii) to reduce the annual random testing rate from 50 percent to 25 percent for most licensee employees (i.e., those that do not perform critical safety- or security-related activities). This risk-informed proposed change is based on an assessment of approximately 35 years of FFD program performance data annually reported to the NRC by licensees and other entities.

The licensee employee workforce has consistently tested positive at much lower rates on pre-access and random drug and alcohol testing than the contractor/vendor workforce. The data show two to three times higher positive rates for contractor/vendors than licensee employees. In addition, FFD program performance data has consistently demonstrated that the licensee employee worker population has very low subversion rates.

The existing 50 percent annual random testing rate would continue to apply to the small subset of licensee employees that perform critical safety and security-related functions (i.e., individuals licensed under 10 CFR part 55, “Operators’ Licenses,” to operate a power reactor, security personnel under § 26.4(a)(5), FFD program personnel under § 26.4(g), and any supervisory personnel directing the operation or maintenance of safety- or security-related SSCs or directing the performance of security duties under § 26.4(a)(5)).

(g) Random testing—use of consortium/third-party administrators

The proposed rule would amend § 26.31(d)(2)(vii) to incorporate a requirement—similar to that described in § 26.607(b)(2)(vi) of subpart M of 10 CFR part 26—that applies to FFD programs with small staff sizes where random testing cannot be implemented without predictability. Small staff sizes can contribute to increased predictability in random testing, due to the possibility for staff to make inferences based on patterns in testing frequency that are more easily recognizable when there is a smaller pool of employees to choose from. For FFD programs with small staff sizes, the proposed rule—under a new § 26.31(d)(2)(vii)(C)—would require the use of a consortium/third-party administrator (C/TPA) to include the workers from multiple licensees or other entities in a combined random testing pool, from which the C/TPA would make testing selections throughout the year. Use of a C/TPA would significantly improve the effectiveness of the random testing programs of potential future licensee sites that may have small worker populations, and would ensure that individuals at these facilities would not be able to predict whether random testing would be conducted in a given period of time. As discussed in the 2026 part 53 final rule, C/TPAs have been used for many years by other Federally-regulated testing programs implemented by the U.S. Department of Transportation, such as those covering independent owner-operator truck drivers. This proposed aligning change would ensure that effective random testing programs can be implemented at future nuclear power reactor sites under parts 50 and 52 that may be operated by a small number of individuals.

The proposed rule would also include a conforming revision to § 26.607(b)(2)(vi) to ensure that a C/TPA-managed random testing pool for a facility licensed under part 53 meets the same annual random testing rate as that required under § 26.607(b)(2)(v). Without this correction, a C/TPA pool would not have a specified random testing rate.

(h) Licensee audits of HHS-certified laboratories

The proposed rule would eliminate the § 26.41(c)(2) requirement for licensees and other entities to annually audit the HHS-certified laboratories maintained under contract to perform testing. These audits are redundant because HHS's National Laboratory Certification Program (NLCP) uses highly trained technical experts to independently inspect each HHS-certified laboratory twice per year. The NLCP inspection process evaluates the majority of laboratory services and functions provided to licensees and other entities under part 26, and the § 26.168 performance-based blind performance testing program (i.e., quarterly submission of BPTSs and implementing of corrective actions under §§ 26.719(c) and 26.167(f)) effectively monitors and addresses unsatisfactory performance issues associated with unique testing program attributes specific to NRC programs. As a result of eliminating the annual auditing requirement, the proposed rule would also make conforming changes to § 26.41(a), (c)(1), (g), and (g)(4) and would remove § 26.41(g)(5). These proposed rule changes would reduce unnecessary regulatory burden on licensees and other entities and the HHS-certified laboratories that perform testing for part 26 regulated entities.

(i) HHS-certified laboratory contract provisions for Subpart M FFD Programs

The proposed rule would revise § 26.607(c)(4), in subpart M of 10 CFR part 26, to align with the requirements of § 26.153(f) that apply to existing licensees and other entities implementing FFD programs under part 26. Paragraph § 26.607(c)(4) requires, in part, that each licensee or other entity establish and maintain a contract with the HHS-certified laboratory relied upon for testing, and that the contract must stipulate that the laboratory is subject to inspection and auditing by the licensee or other entity, and that the laboratory must provide access to records and permit copying and removal of

records, if necessary. However, § 26.607(c)(4), as published in the 2026 final rule that created subpart M, did not include other important contractual requirements in § 26.153(f). The proposed rule would address these differences between the commensurate requirements by creating a new § 26.607(c)(5) that would replace the last sentence currently in § 26.607(c)(4).

Specifically, the proposed rule would add the requirements equivalent to those in the existing requirements of § 26.153(f)(1) through (6). These requirements specify that laboratories must comply with applicable provisions of any State licensor; make qualified personnel available to testify at any administrative or disciplinary proceedings against an individual based on a laboratory's test results; and provide a donor with access, upon written request, to all laboratory records associated with testing of the individual's specimen and any relevant records on laboratory certification, review, or revocation-of-certification proceedings. These requirements also include individual privacy requirements pertaining to laboratory records; conflict of interest provisions applicable to a licensee's or other entity's medical review officer (MRO); and the requirement that the NRC and any licensee or other entity using the laboratory's services must be permitted to inspect the laboratory at any time, including unannounced inspections.

Maintaining uniform contractual requirements for HHS-certified laboratories that perform testing for any licensee or other entity FFD program under part 26 would be necessary because the NRC does not regulate HHS-certified laboratories. As such, contractual requirements would ensure that the NRC and its licensees and other entities have adequate access to each laboratory facility, its personnel, and its records, as necessary to conduct quality assurance reviews. Contractual requirements would also ensure that conflicts of interest do not exist between the laboratory and MROs who may review the laboratory's test results for a licensee or other entity.

(j) Maintaining back-up HHS-certified laboratories under contract for Subpart M FFD Programs

The proposed rule would remove the § 26.607(c)(4) requirement that a licensee or other entity maintain a contract with a back-up HHS-certified laboratory for each biological specimen tested. While a contract with a primary laboratory performing testing on all donor specimens for a licensee or other entity is necessary, imposing a requirement that a back-up laboratory also be maintained under contract is unnecessarily restrictive, inconsistent with industry practice, and is not required for current licensees and other entities implementing an FFD program under part 26.

A back-up HHS-certified laboratory typically conducts testing for a licensee or other entity only when a donor is determined to have violated the FFD policy based on a confirmed positive drug test result or a substituted or adulterated validity test result, and the donor requests retesting at a second laboratory to independently verify the accuracy of the initial laboratory's test result. Many current licensees and other entities implementing FFD programs under part 26 do not maintain a contractual relationship with a particular back-up laboratory and instead provide a donor with a list of all HHS-certified laboratories in the United States to choose from with respect to conducting additional testing on their specimen.

Given the limited use of back-up laboratories by existing licensees, the § 26.607(c)(4) contractual requirement would impose an unnecessary additional burden on future part 53 licensees and other entities that implement subpart M FFD programs and is inconsistent with the current HHS-certified laboratory contractual requirements that apply to part 50 and 52 licensees and other entities. The proposed change would reduce unnecessary regulatory burden and afford donors maximum flexibility in choosing the HHS-certified laboratory to perform additional testing on their specimens, in instances where follow-up testing is requested after an FFD policy violation has been determined.

(k) Licensee testing facilities

The proposed rule would eliminate subpart F, “Licensee Testing Facilities.” Under subpart F, part 26 currently enables licensees to conduct initial drug and initial validity testing on urine specimens at a licensee testing facility (LTF), typically located at the power reactor site. Any specimen tested by an LTF that does not test negative or has a validity testing issue must be forwarded to an HHS-certified laboratory for additional testing.

Historically, LTF testing was the preferred option for many FFD programs because of the quick turnaround time on negative drug test results, which enabled the timely in-processing of workers during outages. Use of LTFs, however, has steadily declined over time as HHS-certified laboratories have greatly improved the turnaround times for reporting negative test results, and no licensee FFD programs currently use an LTF. Operating experience also demonstrates that future use of LTFs is unlikely given high operating costs, the increasing technical complexity of urine testing (e.g., drugs tested, cutoff levels used, validity tests performed), and the fact that LTFs can only test urine specimens.

Eliminating the option for LTFs would improve regulatory effectiveness and efficiency by more closely aligning the part 26 drug testing program with the HHS and DOT testing programs, both of which require testing to be performed at HHS-certified laboratories. Eliminating subpart F would also simplify other part 26 requirements beyond subpart F, because numerous sections reference the use of an LTF or describe LTF-specific processes. Eliminating subpart F would also reduce the administrative burden on the NRC to maintain training programs and inspection procedures that accommodate LTF use.

On December 3, 2025 (90 FR 55621), the NRC published a direct final rule to insert a conditional sunset provision into § 26.121, “Purpose,” and certain other regulations in response to E.O. 14270, “Zero-Based Regulatory Budgeting to Unleash American Energy” (90 FR 15643; April 15, 2025). The conditional sunset provision in §

26.121 provides that subpart F of part 26 will cease to have effect on January 8, 2027, unless the NRC, after considering public input on the costs and benefits of the subpart, determines that the cessation deadline should be extended. The NRC is using this proposed rule to accelerate the sunsetting of subpart F by proposing to remove subpart F and make other conforming changes.

(l) Event notification for supervisor FFD policy violations

The proposed rule would risk-inform the 24-hour reporting requirement in § 26.719(b)(2) to notify the NRC of significant violations of a licensee's or other entity's FFD policy by supervisory personnel. Specifically, the proposed rule would focus this notification requirement on supervisors who direct the operation or maintenance of safety- or security-related SSCs or who direct the performance of security duties as specified in § 26.4(a)(5).

The timely reporting of information to the NRC is necessary to enable prompt regulatory action, if needed. Operating experience demonstrates that 24-hour notification of FFD policy violations for supervisors directing work activity that is not safety- or security-significant is unnecessary. These violations would continue to be captured in the existing annual FFD program performance reporting requirements under §§ 26.717, "Fitness-for-duty program performance data," and 26.417(b)(2), which ensure that the NRC receives uniform and robust information on all FFD program violations. This risk-informed change would reduce unnecessary burden on licensees, other entities, and the NRC.

(m) Behavioral observation program

The proposed rule would apply the same behavioral observation program (BOP) requirement to SAEs that already applies to MROs and MRO staff under § 26.31(b)(1)(v). The change would make SAEs subject to BOP when onsite at a licensee or other entity's facility, removing the current distinction between MROs and MRO staff, who are subject to BOP when onsite, and SAEs, who are currently subject to BOP both onsite and offsite when they are providing services to an FFD program. SAE and MRO

functions are typically, although not always, performed by the same medical professional. Under the current requirements, if a medical professional is both an MRO and an SAE for the same FFD program, that professional is not subject to BOP when performing services for the licensee from an offsite location. However, if that same professional only provided SAE services to a licensee, they would be subject to BOP at whatever location they provided services to that licensee's FFD program. This BOP distinction between MROs and SAEs poses an unnecessary burden on licensees and other entities that choose to use medical professionals that only provide SAE services. SAEs also typically provide services to FFD programs from locations other than a licensee's or other entity's facility, communicating with individuals by telephone or by video teleconference methods. Therefore, this change would reduce unnecessary regulatory burden on licensees and other entities that rely on SAEs that do not also provide services as MROs.

(n) Shy-bladder evaluation

A shy-bladder evaluation is required under current § 26.119, "Determining 'shy' bladder," if a donor is unable to provide a urine specimen of adequate quantity for drug testing within the 3 hours permitted for a urine collection. A shy-bladder evaluation must be completed within 5 business days of the unsuccessful attempt and performed by a licensed physician that is acceptable to the MRO and has expertise in the medical issues raised by the donor's inability to provide a specimen for testing. The proposed rule would revise § 26.119(a) to extend the deadline to complete a shy-bladder evaluation from 5 business days to 10 business days if a justification acceptable to the MRO is provided by the donor.

The purpose of a timely evaluation is to determine if a medical condition precluded the donor from providing a urine specimen for testing (e.g., end stage renal failure). If a medical condition is identified, then the MRO could request the collection of an alternative specimen for drug testing. If no medical condition is identified, then the donor is determined to have subverted the testing process by refusing to provide a urine

specimen for testing. Under the current requirements, if a donor is unable to obtain a medical evaluation within 5 business days, the licensee would make a subversion attempt determination for a refusal to provide a specimen for testing and the individual would be permanently denied authorization under § 26.75, “Sanctions.” The proposed rule would reduce unnecessary regulatory burden by providing additional flexibility to accommodate for potential challenges a donor may encounter in obtaining an appointment and completing the required shy-bladder evaluation by an appropriately qualified physician within 5 business days from the date of failing to provide a specimen for testing. Based on industry operating experience, the NRC anticipates that licensees would only exercise this flexibility on rare occasions, when necessary to address extenuating circumstances.

(o) Initial drug test requirements

The proposed rule would revise paragraph (1) of § 26.167(d), “Quality control requirements for performing initial drug tests,” in three ways. It would remove “of urine” from the phrase “any initial drug test of urine performed by an HHS-certified laboratory,” to clarify that the initial drug testing requirements apply to any specimen that is tested by an HHS-certified laboratory (i.e., urine or oral fluid under § 26.83(b)). It would also remove the requirement that HHS-certified laboratories use an immunoassay “that meets the requirements of the Food and Drug Administration for commercial distribution.” Instead, § 26.167(d)(1) would specify that the initial drug test may be an immunoassay or an alternate technology that is permitted for use in Federal workplace drug testing programs to align with changes to Section 11.10 of the HHS Guidelines (82 FR 7920; January 23, 2017). The proposed rule would also remove the prohibition that “non-instrumented immunoassay testing devices that are pending HHS/SAMHSA [Substance Abuse and Mental Health Services Administration] review and approval may not be used for initial drug testing under this part.” This prohibition is unnecessary because the requirements in § 26.167(d)(1) are specific to testing performed at HHS-certified laboratories, which adhere to the testing requirements in the current version of

the HHS Guidelines for the specimen(s) to be tested, unless otherwise directed under part 26. Reducing the prescriptive nature of the initial drug testing requirement would reduce unnecessary regulatory burden and ensure that licensees and other entities can benefit from the best testing approaches available at HHS-certified laboratories to identify drugs and drug metabolites. The proposed rule would also make conforming changes to § 26.405(f) in subpart K.

(p) MRO qualifications

Under paragraph (a) of § 26.183, "Medical review officer," an MRO must be a physician holding either a Doctor of Medicine or Doctor of Osteopathy degree who is licensed to practice medicine by any State or Territory of the United States, the District of Columbia, or the Commonwealth of Puerto Rico. The proposed rule would revise § 26.183(a) to clarify that "an equivalent foreign degree" also would be acceptable. This clarification would ensure that physicians who have received their medical degrees from medical schools outside the United States could still be considered qualified to serve as an MRO under part 26. This change would reduce unnecessary regulatory burden on licensees and other entities by allowing them to consider additional qualified physicians who may be able to provide services as an MRO.

(q) Review of dilute specimen test results

The proposed rule would address inconsistencies in the requirements that apply to the review of dilute test results to clearly define the activities that must be performed by MROs and that may be performed by MRO staff.

As currently written in § 26.183(c), one of the responsibilities of the MRO is to review and interpret dilute test results, and § 26.185(g)(2) and (4) specify how the MRO is to conduct the reviews of those results. For MRO staff, § 26.183(d)(2)(ii) limits the review of dilute test results to performing administrative functions (e.g., reviewing custody and control forms for errors). However, under § 26.183(d)(2)(i), MRO staff under the direction of the MRO are permitted to "receive, review, and report negative test results to the licensee's or other entity's designated representative." As currently written,

the MRO must review all dilute test results (both positive and negative), which is inconsistent with the MRO review requirements for dilute test results under § 26.185(g)(2) and (4). Specifically, § 26.185(g)(2) states that MRO review is required for "positive and dilute" specimen test results, and § 26.185(g)(4) states that MRO review is not required for "negative and dilute" specimen test results. A "negative and dilute" test result is not an FFD policy violation and is therefore acceptable for review by MRO staff under § 26.183(d)(2)(i).

The proposed rule would make changes to § 26.183(c) and (c)(1), § 26.183(d)(2)(ii) through (iv), and § 26.185(b) by replacing "dilute" with "positive and dilute." The proposed rule would also make the conforming change of adding the term "positive and dilute" to § 26.405(g). These changes would reduce unnecessary regulatory burden by addressing internal inconsistencies in the part 26 requirements regarding the review of dilute positive and dilute negative validity test results.

(r) Clinical evidence of abuse before verifying positive results for using another person's prescription medication

The proposed rule would enable licensees to more efficiently address the misuse of controlled substances by individuals by allowing licensees to more readily address instances wherein an individual illegally uses a prescription medication that has not been prescribed to them.

Currently, under § 26.185(j)(3), if the MRO determines that a donor has used another individual's prescription medication and no clinical evidence of drug abuse is found during the required clinical examination, the MRO must report that the donor misused a prescription. However, under the current framework, this is not considered a positive test result. The MRO is to report an FFD policy violation for a confirmed positive test result only when clinical evidence of abuse also exists.

Requiring the MRO to confirm a positive test result only if clinical evidence of drug abuse exists, even when the donor admits to using another individual's prescription medication and lacks a legitimate medical explanation, is inconsistent with the HHS

Guidelines and DOT requirements. Specifically, under those programs, the MRO is to report a confirmed positive drug test result if a donor admits to unauthorized use of a drug or does not provide a legitimate medical explanation for the test result (i.e., a valid prescription, as specified in Section 13.5 of the HHS Guidelines for urine and oral fluid testing and in DOT's requirements in 49 CFR 40.137).

The use of another person's prescription medication is prohibited by Federal law and is described in the HHS "Medical Review Officer Manual for Federal Workplace Drug Testing Programs (effective February 1, 2024)." Specifically, the MRO Manual states that—

> Under no circumstances can prescriptions be legally transferred from a different individual to a donor in the event the donor exhausts his or her own prescription medication, even if the other individual's medication is identical and prescribed for the same medical condition (Controlled Substances Act Revised 2010, Pharmacist's Manual, Section VIII—Dispensing Requirements—Required Information for Prescription Labels). Federal Food and Drug Administration regulations [found in 21 CFR 290.5] require that the label of any drug listed as a "controlled substance" in Schedules II, III, or IV of the [Controlled Substances Act] must, when dispensed to or for a patient, contain the following warning: "CAUTION: Federal law prohibits the transfer of this drug to any person other than the patient for whom it was prescribed."

The proposed rule would eliminate the requirement in § 26.185(j)(3) to determine that clinical signs of abuse exist to report a positive test result as an FFD policy violation when a donor admits to using another individual's prescription medication. This proposed rule change would align with other Federal agency testing policies, would improve public health and safety and common defense and security by allowing licensees to more efficiently address known trustworthiness and reliability concerns, and would remove unnecessary regulatory burden, as a positive test result could be reported by an MRO after a discussion with the donor (i.e., without the need to perform a clinical evaluation).

(s) SAE credential—State-licensed or -certified marriage and family therapists

The proposed rule would add a State-licensed or -certified marriage and family therapist (MFT) to the list of credentials that would qualify individuals to serve as an SAE under § 26.187(b). This action would address the PRM docketed as PRM-26-4.

To be a State-licensed or -certified MFT requires a master's or doctoral degree, supervised clinical experience, and successful completion of the national examination conducted by the American Association for Marriage and Family Therapy Regulatory Board. Many programs accredited by the Commission on Accreditation of Marriage and Family Therapists have "substance abuse" knowledge as part of their core curriculum requirements in their graduate studies. Potential candidates can sit for the examination only after their credentials have been examined and found to meet the education and experience requirements for licensure or certification in their respective States. In 2006, the DOT added State-licensed or -certified MFTs to its list of credentialed professionals eligible to serve as substance abuse professionals under 49 CFR 40.281(a) (71 FR 49382; August 23, 2006).

Updating the § 26.187(b) SAE credential list to include State-licensed or -certified MFTs would be consistent with the approach taken by the NRC when it established the SAE requirements in the 2008 part 26 final rule. In the 2008 part 26 final rule, the NRC stated that it had adapted many of the SAE provisions from the DOT requirements regarding substance abuse professionals under 49 CFR part 40, subpart O.

This proposed change would reduce unnecessary regulatory burden by allowing licensees and other entities to consider additional qualified individuals who may be able to provide SAE services.

(t) SAE credential—Certified Addiction Specialist by the American Academy of Health Care Providers in Addictive Medicine

The proposed rule would address a PRM (PRM-26-7) that requested that the "Certified Addiction Specialist" (CAS) certification from the American Academy of Health Care Providers in the Addictive Disorders (the Academy) be added to the list of

acceptable credentials to serve as an SAE under § 26.187(b)(5). In a supplement to its petition to the NRC dated August 3, 2011 (ML11256A020), the Academy stated that it was in the process of preparing a petition to request that the DOT add the CAS certification to the substance abuse professional credentials in 49 CFR 40.281(a). As of the issuance of this proposed rule, however, the CAS credential does not appear on the DOT's approved credentials list in 49 CFR 40.281(a), and the NRC has not received any additional information to support the Academy's petition. Furthermore, the NRC evaluated publicly available information regarding the CAS credentialling process and determined that, while the training and education requirements are similar to those in place for credentials currently accepted in accordance with NRC requirements, the Academy did not provide adequate information on the examination process associated with the CAS credential. Based on this evaluation, the NRC determined that there is insufficient information available to support adding the CAS certification to the list of acceptable credentials. The proposed rule, therefore, would not incorporate the CAS certification into § 26.187(b)(5).

(u) Face-to-face for-cause determinations of fitness

The proposed rule would remove the prohibition on the use of electronic means to perform face-to-face for-cause determinations of fitness under § 26.189(c), because video technology has advanced significantly since the creation of the § 26.189(c) requirement in the 2008 part 26 final rule.

Video teleconference technology is already being used by some clinicians to complete other NRC-required evaluations, such as performing psychological assessments under the personnel access authorization requirements in § 73.56(e)(4) or determinations of fitness performed under § 26.189(b) when potentially disqualifying FFD information is discovered about individuals subject to part 26.

The proposed rule would specify that if video teleconference technology is used by a professional to conduct a face-to-face determination of fitness for a for-cause drug and alcohol testing determination under § 26.31(c)(2) or a fatigue assessment performed

for cause under § 26.211(a)(1), then the determination must be supported by an individual that is in the room with the person being evaluated. A supporting person would be necessary in these circumstances to ensure that the professional performing the determination of fitness is provided with contemporaneous information that can only be obtained in the location where the person is being assessed (e.g., sensory information such as the smell of alcohol on an individual's breath or an aspect of the individual's physical condition that is not ascertainable by video teleconference). The proposed rule would specify that the supporting person must have received training on the FFD program under § 26.29, which includes the "ability to observe and detect performance degradation, indications of impairment, or behavioral changes." All individuals subject to a licensee's or other entity's FFD program must complete this training.

Eliminating the prohibition on the use of electronic communications to perform face-to-face determinations of fitness would reduce unnecessary regulatory burden and could improve the speed at which these determinations are made.

(v) Post-event testing terminology

The proposed rule would make a conforming change to terminology used in § 26.405(c)(3) that applies to FFD programs implemented under subpart K of part 26. Specifically, the proposed rule would replace "post-accident" with "post-event" and "accident" with "event." The term "post-event" is used in FFD program requirements under subpart M of part 26. The term "post-event" is also used in NRC Forms 890, "Single Positive Test Form," and 891, "Annual Reporting Form for Drug and Alcohol Tests," which licensees and other entities have used to submit FFD program performance data to the NRC under § 26.417(b)(2).

(w) Clarification of Subpart K FFD program applicability to individuals directing the construction of safety- or security-related SSCs

The proposed rule would clarify the provisions of § 26.419, "Suitability and fitness evaluations," for individuals who direct the construction of safety- or security-related

SSCs in subpart K FFD programs to ensure that licensees are able to assign duties to those individuals in accordance with FFD program requirements.

Section 26.4(f) requires that individuals constructing or directing the construction of safety- or security-related SSCs be subject to a subpart K FFD program (or an FFD program that meets all the requirements of part 26, except for subparts I, K, and M). Furthermore, in the 2008 part 26 final rule, the Commission stated that § 26.419 "requires licensees and other entities who implement FFD programs under subpart K to develop, implement, and maintain procedures for evaluating whether to assign individuals to the duties specified in § 26.4(f)." However, the rule text of § 26.419 only includes provisions for assigning duties to "individuals to construct safety- and security-related SSCs," but does not currently include such provisions for the individuals directing those activities. As such, the NRC is proposing to include in § 26.419 individuals directing the construction of safety- or security-related SSCs to provide clarity and maintain consistency with § 26.4(f) and the intent of the 2008 part 26 final rule.

(x) Terminology clarification for construction FFD programs

The proposed rule would make a conforming change to the terminology used in § 26.401(b), revising the term "entities" to "licensees and other entities." This administrative revision would provide consistency in the use of the terminology across part 26, subpart K.

(ii) Fatigue Management

(a) Temporary relief from work hour controls

The NRC is proposing to add a new exception from the work hour controls in § 26.205(c) and (d) during sequestration events as an alternative to licensees needing to grant waivers. This new exception in § 26.207(e) would address sequestration events during which licensee personnel remain on-site at the facility due to unavoidable external conditions (e.g., a severe weather event, public health emergency, or failure of local infrastructure) that could affect safe and secure plant operation. Part 26 currently contains exceptions for plant emergencies and other limited circumstances but does not

account for conditions in which personnel may be required to remain on site due to unavoidable external circumstances.

Under the proposed rule, during such events, licensees would be able to implement alternative fatigue management controls for up to 60 days, consistent with those authorized by the NRC during the COVID-19 public health emergency (e.g., NRC Letter, “Quad Cities Nuclear Power Station, Units 1 and 2 – Exemption from Select Requirements of 10 CFR Part 26 (EPID L-2020-LLE-0018 [COVID-19]),” dated April 8, 2020). If a licensee were to use this exception and need to extend the alternative controls beyond 60 days, the licensee would need to submit an exemption request. The addition of the sequestration exception would provide a less burdensome alternative to waivers or exemption requests during sequestration events.

(b) Annual fatigue reporting

The NRC is proposing to eliminate the requirement in § 26.203(e) and § 26.717(b)(9) for licensees to provide annual reports of waivers and fatigue management program information to the NRC. In addition, the NRC is also proposing to eliminate the same requirement for subpart M FFD programs in § 26.202(e). Annually, the FFD performance reports have included limited instances when waivers to the work hour controls were issued, with the trends decreasing in the years since the requirements were first implemented in 2009, demonstrating the successful implementation of the work hour controls to mitigate fatigue. While no longer submitted in an annual report, the associated records would continue to be maintained by licensees in accordance with § 26.203(d) and would be available for NRC inspection or review as needed. The elimination of the reports would reduce burden on licensees and would also save NRC resources associated with the receipt and maintenance of these records.

(c) Expanding the applicability of remote assessments

The NRC is proposing changes to §§ 26.207(a)(1)(ii) and 26.211(b) to allow additional licensees to use electronic communications to perform face-to-face

assessments to support the approval of work hour control waivers and to conduct fatigue assessments. Under the current provisions, only licensees and other entities under 10 CFR part 53, as specified in § 26.3(f), can use electronic communications for these purposes. The proposed changes would expand the option of using electronic communications to other types of NRC licensees specified in § 26.3(a), (c), and (d). The provisions would continue to indicate that supervisors may conduct such assessments from a remote location under appropriate circumstances, and that such remotely conducted assessments need to be supported by someone who is present in-person with the individual being assessed and who is trained in accordance with the requirements of either §§ 26.29 and 26.203(c), or §§ 26.608 and 26.202(c).

The reasoning for these changes and the associated need for in-person support to augment electronic communications is addressed further in the discussion of the proposed changes to § 26.189(c) in Section IV.A.(i)(u) of this document.

(iii) Changes to Definitions in Part 26

The proposed rule would add two new definitions, revise five definitions, and remove four definitions in § 26.5. The additions, revisions, and removals would improve the clarity, consistency, and accuracy of the requirements under part 26. Specifically, this proposed rule would add definitions for “Escort” and “Sequestration event.” In conjunction with another proposed rule change to remove subpart F, “Licensee Testing Facilities,” this proposed rule would revise definitions for “Analytical run,” “Cancelled test,” “Cutoff level,” “Positive result,” and “Rejected for testing”; and remove definitions for “Licensee testing facility,” “Questionable validity,” “Validity screening test,” and “Validity screening test lot.”

A definition for “Escort” would be added, defining the term to mean a person who is designated by the licensee or other entity to be responsible for directly observing an individual who has been assigned to perform duties and responsibilities or maintain the type of access described in § 26.4(f) but is not subject to the requirements in part 26.

A definition for “Sequestration event” would be added, defining the term to mean a situation in which personnel remain on-site at a nuclear power reactor due to unavoidable external conditions that pose a risk to the safe, secure, and continuous operation of the facility.

B. Security Requirements for Independent Spent Fuel Storage Installations (ISFSIs) (Parts 72 and 73)

An ISFSI is a complex designed for the safe storage of power reactor spent nuclear fuel and certain other radioactive materials. These installations use robust storage systems, such as dry casks, that securely contain and shield the radioactive material until it can be disposed of in the future, allowing licensees to store this material safely on site or at standalone storage locations. The security risk profile of an ISFSI is reduced from that of an operating nuclear power reactor due to the absence of a fueled reactor and the placement of all spent fuel into these robust storage systems. This configuration eliminates reactor-related target sets and significantly lowers the potential consequences of radiological sabotage.

There are two main types of ISFSIs regulated by the NRC: general license ISFSIs and specific license ISFSIs. A general license ISFSI is operated by a nuclear power plant licensee under a general license provided in NRC regulations. Section 72.210, “General license issued,” states that a general license for an ISFSI is issued to persons authorized to possess or operate nuclear power reactors under 10 CFR part 50, part 52, or part 53. A nuclear power plant licensee does not need to apply for a separate, stand-alone license for the ISFSI. In contrast, a specific license ISFSI is authorized through a separate, detailed licensing process that is independent from the nuclear power reactor license. Although both types of ISFSIs must meet NRC safety and security standards, there are differences in the licensing approach and in some of the security requirements that currently apply to each type.

The proposed requirements for ISFSI security would enhance consistency and regulatory clarity between general and specific license ISFSIs. Licensees operating

general license ISFSIs that are not collocated with an operating reactor would have the option to provide physical protection under the same requirements that apply to specific license ISFSIs. These changes would provide consistency for similarly situated ISFSIs, while reducing the burden of submitting exemption and alternative measure requests.

Additionally, this proposed rule would extend the time associated with submitting ISFSI security plan changes to the NRC. The frequency required for the submission of security plan changes would be modified to reduce the licensee burden that is associated with security plan revisions.

(i) Security Requirements for ISFSIs Located Outside a Reactor's Protected Area

The proposed rule would include changes addressing security requirements for ISFSIs located either outside the protected area (PA) of an operating reactor or within the PA of a decommissioning reactor for which all spent fuel at the site has been placed in dry storage.

Some ISFSIs are located within the same PA as an operating reactor. Other ISFSIs are located in a separate PA because either the reactor with which an ISFSI was originally collocated has gone into decommissioning or the ISFSI was constructed with a separate PA. The proposed changes to parts 72 and 73 of the NRC's regulations would allow licensees with ISFSIs in this latter category the option to implement security requirements that are designed specifically for ISFSIs. With regards to ISFSIs adjacent to decommissioning reactors, the proposed changes are consistent with those in SECY-24-0011, "Final Rule: Regulatory Improvements for Production and Utilization Facilities Transitioning to Decommissioning," dated January 31, 2024, which is currently being considered by the Commission.

This proposed rule would revise § 72.212(b)(9) to allow general license ISFSIs the option to develop and implement their physical protection programs in accordance with § 73.51, "Requirements for the physical protection of stored spent nuclear fuel and high-level radioactive waste," instead of § 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage." This

change would align the physical protection requirements of general license ISFSIs and specific license ISFSIs for separate protected areas constructed outside the PA of an existing operating reactor, or during decommissioning, once all spent fuel at the site has been placed in dry storage. This change would be appropriate because the security requirements in § 73.51 are designed for and provide security appropriate to the reduced risk level of ISFSIs as compared to nuclear power plants, which are subject to § 73.55. This change would reduce the regulatory burden on current and future licensees by offering the increased flexibility provided under § 73.51. In particular, licensees that choose to transition to § 73.51 would no longer be required to implement protection measures against the design basis threat nor comply with the associated requirements outlined in § 73.55.

The proposed rule also includes conforming changes to §§ 72.13, “Applicability,” and 73.51 to clarify the applicability of the security requirements that are found in part 72, subpart H, “Physical Protection,” to general license ISFSIs. Currently, these licensees need to submit alternative measures or exemption requests from certain § 73.55 requirements to allow for the implementation of security requirements that are consistent with the risk profile for their facilities. The proposed change would eliminate the need to submit alternative measures or exemption requests. Licensees that elect to implement the new proposed regulatory requirements would provide a revised security plan through the process described in paragraph (p)(2) of § 50.54, “Conditions of licenses.”

ISFSIs that are within an operating reactor PA would still be required to implement § 73.55, consistent with the physical protection program for the reactor, with the specific exceptions in § 72.212(b)(9). Additionally, licensee physical protection programs would be required to continue to address the terms of any applicable security-related orders associated with either a general or specific license ISFSI.

(ii) Submittal of Security Plan Changes

The proposed rule would extend the time associated with the requirement to submit ISFSI security plan changes to the NRC under paragraph (e) of § 72.44, “License conditions,” and paragraph (b) of § 72.186, “Change to physical security and safeguards contingency plans.” Instead of submitting to the Commission a report containing a description of each change within two months after the change is made, licensees would have to submit the report within 12 months after the change is made. This revision would reduce the licensee burden that is associated with security plan revisions. The extension would also maintain safety and security because it would be limited to reports of changes that would not decrease the effectiveness of the plans.

C. Physical Security Requirements (Part 73)

Under this proposed rule, the security regulations for the physical protection of plants and materials under 10 CFR part 73, along with their associated guidance documents, would be revised to reduce unnecessary burdens and respond to credible risks—as directed in E.O. 14300, section 5(g)—to support efficiencies in licensing and oversight. Where possible, prescriptive requirements would be replaced with more performance-based requirements to streamline, clarify, and modernize the current regulations, thus increasing flexibility for current and future licensees and facilitating the increased deployment of new civilian nuclear reactor technologies, consistent with section 2(b) of E.O. 14300.

This proposal covers updates across various elements of part 73, including physical protection, security training, access authorization, and cybersecurity for power reactors; transmittal of safeguards information (SGI); special nuclear material security; records; and definitions. This proposal also incorporates changes to part 73 intended to address industry concerns from the 2023 Enhanced Weapons final rule, the consideration of law enforcement support to licensee security programs, and certain aspects of the draft final decommissioning rule in SECY-24-0011.

(i) Power Reactor Physical Protection Program

The proposed changes to § 73.55, as well as appendices B, “General Criteria for Security Personnel,” and C, “Licensee Safeguards Contingency Plans,” to part 73, would support the agency’s mission to enable the safe and secure use and deployment of civilian nuclear energy technologies and would reduce unnecessary burden on current and future licensees.

This proposed rule would provide licensees with increased flexibility in implementing their physical protection programs by incorporating performance-based requirements and, where appropriate, allowing for specific alternatives. The proposed alternatives would most likely be available to non-light water reactor designs that incorporate security by design and engineered safety or security features.

For the existing light-water reactor fleet, the proposed revision of the security requirements would eliminate certain prescriptive requirements that are more appropriately addressed in regulatory guidance and in some instances are no longer necessary for the implementation of the physical protection program.

This proposed rule would establish a revised performance objective that applies a risk-informed approach that would continue to provide reasonable assurance that activities involving special nuclear material are not inimical to the common defense and security, and do not pose an unreasonable risk to public health and safety.

Existing licensees that are in compliance with § 73.55 as of the effective date of publication of the final rule, if this proposed change is made effective in a final rule, would also be in compliance with the proposed revisions to the regulations and would not be required to modify their current physical protection programs. However, existing licensees would be able to voluntarily adopt the proposed alternative methods of compliance and take advantage of the increased flexibility in implementing the requirements of § 73.55.

This proposal builds on previous efforts to risk-inform physical security regulations by shifting from prescriptive to performance-based requirements to allow for

the use of technology-neutral alternatives (e.g., security and safety features) in the implementation of § 73.55. The core performance-based criteria for implementing licensees' physical protection programs would remain unchanged because these programs would continue to be required to detect, assess, interdict, and neutralize threats.

The proposed amendments would revise § 73.55 and appendices B and C to 10 CFR part 73 to enhance requirements for physical protection, power reactor security training, and contingency response. Specifically, the proposed revisions should provide increased flexibility in the implementation of security, training, and response measures. This would be accomplished by modifying the performance objective, the use of performance-based requirements, and the use of voluntary alternatives that allow for the use of technology and engineered design features.

The proposed requirements would adopt technology-inclusive approaches to provide the necessary regulatory flexibility for licensing and regulating multiple categories of nuclear reactor technologies and designs. A technology-inclusive approach to security requirements would provide greater flexibility in both the design and implementation of physical protection programs. Licensees and applicants using this approach could integrate security considerations into the safety design process, enabling the effective implementation of security measures through the use of both design-based and engineered security features. This approach could enable safety and security functions to work collaboratively in the implementation of the physical protection program. Additionally, the proposed technology-inclusive approach would allow for the increased use of technology by licensees to implement security measures for the protection of a facility, providing greater operational flexibility.

(a) High assurance

The general performance objectives throughout part 73 would be revised to reflect the Commission's decision on the concept of "high assurance" as it relates to licensee physical protection programs. In SRM-SECY-16-0073, "Staff Requirements—

SECY-16-0073—Options and Recommendations for the Force-on-Force Inspection Program in Response to SRM-SECY-14-0088," dated October 5, 2016, the Commission determined that the concept of "high assurance" in security regulations is functionally equivalent to "reasonable assurance" used in safety contexts and that security regulations should not be applied using a "zero risk" mentality. Therefore, the proposed rule would revise the regulations in §§ 73.20(a), 73.22(f)(3), 73.51(b)(1), 73.54(a), 73.55(b)(1), and 73.56(c) to use the term "reasonable assurance" in place of "high assurance."

(b) Significant core damage and spent fuel sabotage

The performance objective in § 73.55(b)(3) would be revised from specifically protecting against significant core damage and spent fuel sabotage to a broader goal of preventing a release of radionuclides from any source that exceeds the dose reference values defined in § 50.34(a)(1)(ii)(D)(*1*) and (*2*), § 52.79(a)(1)(vi)(A) and (B), or § 53.210, as applicable. This shift would emphasize radiological sabotage in general, rather than focusing solely on core damage or spent fuel scenarios. The existing fleet of light-water reactors would be in compliance with this proposed performance objective by continuing to prevent significant core damage and spent fuel sabotage. The revised objective would be technology-inclusive, providing flexibility to accommodate multiple categories of nuclear reactor technologies and designs, including those that may not have conventional cores.

(c) Achievable target sets

This proposed rule would introduce a revised set of requirements in § 73.55(f), "Target sets," that adopts a risk-informed, technology-inclusive, and graded approach through the identification of achievable target sets. Licensees that voluntarily elect to implement the revised performance objective would need to perform an analysis to identify the necessary plant equipment, operator actions, mitigative measures, detection capabilities, assessment processes, and armed response needed to identify the achievable target sets for the site's physical protection program, which must be designed

to prevent a radionuclide release from exceeding the dose reference values specified in § 50.34(a)(1)(ii)(D)(*1*) and (*2*), § 52.79(a)(1)(vi)(A) and (B), or § 53.210, as applicable, to protect against the design basis threat of radiological sabotage as stated in § 73.1.

Achievable target sets would be identified through a site-specific analysis. Achievable target sets would include those that are within the capabilities of the design basis threat adversary to compromise, destroy, or render non-functional; cannot be mitigated after adversary interference is precluded and prior to a release of radionuclides exceeding the dose reference values defined in in § 50.34(a)(1)(ii)(D)(*1*) and (*2*), § 52.79(a)(1)(vi)(A) and (B), or § 53.210, as applicable; and, if defeated, result irreversibly in exceedance of the dose reference values defined in in § 50.34(a)(1)(ii)(D)(*1*) and (*2*), § 52.79(a)(1)(vi)(A) and (B), or § 53.210, as applicable.

Under this framework, licensees would determine the applicability of § 73.55 as follows:

- If a licensee could demonstrate that no achievable target sets exist, and would not credit any active measures (e.g., operator action, mitigative action, detection, assessment, armed response), then the licensee would be exempt from the remaining requirements of § 73.55. The requirements of 10 CFR part 26; 10 CFR part 37, “Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material”; and §§ 73.21, “Protection of Safeguards Information: Performance requirements,” 73.22, “Protection of Safeguards Information: Specific requirements,” 73.23, “Protection of Safeguards Information—Modified Handling: Specific requirements,” 73.54, “Protection of digital computer and communication systems and networks,” 73.56, “Personnel access authorization requirements for nuclear power plants,” and 73.67 would need to be implemented as applicable.

- If a licensee could demonstrate that no achievable target sets exist, and would credit active measures in making that demonstration, then the licensee would be required to implement the applicable requirements of § 73.55 through its physical security plan, training and qualification plan, safeguards contingency plan, and

cybersecurity plan. Licensees that would rely on active measures could limit the scope of their physical protection program by ensuring that the credited active measures will be implemented when needed in response to threats.

- If a licensee could demonstrate that achievable target sets exist, then the licensee would be required to implement the requirements of § 73.55 through its physical security plan, training and qualification plan, safeguards contingency plan, and cybersecurity plan.

(d) Prescriptive requirements revised to performance-based requirements

The current physical security requirements use a combination of performance criteria (e.g., protection against the design basis threat for radiological sabotage as stated in § 73.1) and numerous prescriptive requirements to implement a physical protection program to achieve the current performance objective. In this performance-based proposed rule, physical security would be implemented through performance criteria to meet the general performance objective, thus giving the licensee flexibility to determine how to meet the established performance criteria for an effective physical protection program. The proposed rule would remove a number of prescriptive requirements while preserving the effectiveness of the physical protection program framework. Power reactor physical protection programs would continue to address each of the programmatic functions of the overall physical protection program (e.g., detection and assessment, delay barriers, armed response, etc.) to meet the performance objectives of 10 CFR 73.55 to protect against the design basis threat of radiological sabotage. For new applicants, the NRC would evaluate the measures an applicant proposes to use to meet the performance criteria and the general performance objective through the NRC's review and approval of the physical security plan. For existing licensees who make changes to their physical protection programs based on the revised performance criteria, the NRC would verify the adequacy of the licensee's measures through inspection.

1. Physical Barriers

Prescriptive physical barrier requirements in current § 73.55(e) would be revised to remove the details concerning the specific considerations and criteria for each barrier, including isolation zones. Isolation zones have been removed from the requirements to provide greater flexibility for licensee programs implementing detection measures. In certain conditions, these clear areas are not necessary to meet detection and assessment requirements due to site-specific configurations. Additionally, advancements in detection and assessment technologies have significantly reduced, or eliminated, the need for clear areas to identify unauthorized access into protected areas. The proposed rule would continue to require licensees to detect attempted or actual penetrations using detection and assessment equipment capable of meeting the performance objectives outlined in 10 CFR 73.55(b).

These specifics would be retained in guidance as voluntary considerations for licensee physical protection programs. Licensees would still be required by proposed § 73.55(e)(1) to ensure that physical barriers are sufficient to meet the performance criteria (e.g., detect, delay, and deter) and performance objective for their intended function.

2. Access Control Measures

Access control measures in current § 73.55(g) would be revised to remove the prescriptive requirements regarding access to different areas of a facility. These specifics would be retained in guidance as voluntary considerations for licensee physical protection programs. Licensees would still be required by proposed § 73.55(g)(1) to ensure that their access control measures meet the performance criteria (e.g., restricts unauthorized access and implements verification measures) and performance objective.

3. Search

The specific methods for how vehicles, materials, and personnel are searched in current § 73.55(h) would be revised with performance criteria applicable to searches conducted in various areas (e.g., owner controlled and protected areas) of licensee

facilities. Under proposed § 73.55(h), licensees would have the flexibility to determine the search method(s) used to meet the performance criteria for conducting searches.

4. Detection and Assessment

Prescriptive detection and assessment requirements in current § 73.55(i) would be revised to allow licensees the flexibility to use technology for surveillance and illumination to meet the performance criteria to detect and assess at all times. Advanced technology systems provide flexible capabilities to licensees offering superior detection range, accuracy, and reliability compared to human observation under 0.2 foot-candle illumination. Replacing a prescriptive lighting level with a technology-based detection strategy aligns with the performance-based approach. Because modern technologies provide detection and assessment capabilities that meet or exceed those enabled by the historical lighting and surveillance requirements, the overall security posture would continue to satisfy the standard of reasonable assurance of adequate protection against radiological sabotage. This proposed change would support the effective implementation of the licensee's protective strategy by allowing site-specific applications that align with the licensee's facility layout and operational needs.

5. Response Requirements

Current requirements in § 73.55(k) identify the minimum number of ten armed responders to implement a site's protective strategy to meet the performance objective to protect against the design basis threat of radiological sabotage. The proposed rule would remove this prescriptive number, allowing licensees flexibility to determine the minimum number of armed responders necessary to implement the site protective strategy and respond to the design basis threat of radiological sabotage. The proposed requirements would continue to allow licensees to use armed responders and armed security officers to form an armed response team to meet response requirements. The proposed rule would add an alternative in § 73.55(k)(5) for current and future licensees that voluntarily elect to rely partially or solely on law enforcement or other offsite armed response personnel to meet the response requirements for their facilities. Licensees that

rely solely on law enforcement or offsite armed responders would be required to obtain prior Commission approval before using these entities to meet the site response requirements.

6. Safety/Security Interface

The NRC proposes to remove § 73.58, “Safety/security interface requirements for nuclear power reactors,” from part 73 to streamline requirements and to eliminate rule text that provides a level of detail more appropriate for guidance. A performance-based requirement for safety/security interface would be added to § 73.55(l)(1). The proposed safety/security interface requirement would require licensees to evaluate and manage changes to safety and security activities to prevent or mitigate potential adverse effects that could impact plant safety or security at power reactors.

The current requirements in § 73.55(l) regarding physical protection for reactor facilities using mixed-oxide (MOX) fuel would be removed. These provisions have never been applied to any applicant or licensee.

7. Security Program Reviews

The prescriptive requirements for conducting a security program review at a periodicity of every 24 months in current § 73.55(m) would be revised to allow a licensee to conduct risk-based security reviews that are commensurate with the importance or significance to the safety of plant operations.

(e) Flexibility in implementing an acceptable physical protection program

The proposed rule would revise § 73.55 to be more technology-inclusive. Designed-in features, structures, systems, and components, as well as engineered and administrative controls, could be used to provide flexibility in implementing an acceptable physical protection program for different reactor designs.

(f) Alternatives

In several areas of the proposed requirements, licensees would be provided with voluntary alternatives to existing regulations to achieve the required performance objectives. These alternatives would be technology neutral (i.e., to address various

approaches to plant SSCs, designs, and technology). The voluntary alternatives might not be suitable for a licensee to implement in all cases; therefore, in determining the use of the voluntary alternatives, licensees would be required to complete a site-specific analysis to determine if their plant design and physical protection program would meet the applicable proposed requirements and the overall performance objective of reasonable assurance of adequate protection against threats up to and including the design basis threat of radiological sabotage. The NRC has provided draft regulatory guidance that describes some acceptable methods to meet the proposed alternatives. Voluntary alternatives have been proposed for the security organization, bullet resistant barriers, Performance Evaluation Program, physical barriers, and response requirements. In addition to the alternatives specifically provided for in the regulations, licensees would be able to continue to propose alternative measures under the provisions of § 73.55(r), “Alternative measures.”

Licensees that retain their current physical protection program would be able to elect to change their security plans and implementing procedures to reference the new proposed regulatory requirements through the § 50.54(p) process.

(g) Appendix B to Part 73

The NRC proposes to revise the general criteria for security personnel in 10 CFR part 73, appendix B, to address the minimum age for employment, for the use of a qualified training instructor for the attestation of training documentation, and to provide flexibility for the use of a nationally recognized course of fire for all weapons identified in this appendix. For the security training that is outlined in appendix B, sections I through VI, the majority of prescriptive requirements would be removed. The requirements for suitability would be streamlined for all security personnel that are identified in appendix B to part 73. Also, the NRC proposes changes to the training for power reactor licensees in the implementation of licensee Performance Evaluation Programs. The proposed rule would reduce the required frequency of tactical response drills from four per year to two per year. In addition, the requirement for each member of each shift to participate in one

force-on-force exercise annually would be modified to once every three years. The proposed modifications to the performance evaluation program reflect that licensees have mature, established training programs that have consistently demonstrated that licensee security forces maintain the knowledge, skills, and abilities for effective contingency response. Tactical response drills would continue to be based on target set scenarios and would provide a practical demonstration of defense against specific design basis threat attributes. The proposed adjustment to the frequency of participation in the licensee's full-scale force-on-force exercises recognizes that full-scale exercises are the most resource intensive to conduct. While valuable, this activity is only one component of a comprehensive performance evaluation program. This proposed change recognizes that the broader performance evaluation program is sufficiently robust without relying on annual force-on-force participation. On an annual basis, licensees would conduct at least one fully integrated force-on-force exercise to test the protective strategy as a whole. The licensee's performance evaluation program would continue to ensure that any degradation in security force member performance and potential protective strategy deficiencies would be identified and corrected through the corrective action program. Additionally, several prescriptive training requirements would be removed from appendix B to part 73 (e.g., range activities periodicity, written exams, required courses of fire, and on-the-job training hours). Removing these prescriptive elements would not eliminate these training areas from the licensee's training and qualification program, rather it would provide licensees with increased flexibility to design and implement training that more directly supports their operational needs. In place of the prescribed range activity periodicity and courses of fire, the regulations would require licensees to ensure security officers have the appropriate types of weapons training at frequencies that ensure the proper handling of firearms with the accuracy that is necessary to implement the use of assigned weapons. This approach allows for flexibility in scheduling and allows the licensee to use performance data to determine the appropriate type of training and intervals, thus reducing administrative burden and

providing for more efficient allocation of resources. With regard to written exams, such exams are only one method of evaluating security force knowledge. The proposed removal of required written exams would allow licensees the option to use other types of knowledge-based activities or performance-based evaluations to evaluate the knowledge, skills, and abilities of members of the security organization. These changes are being proposed to decrease the burden in implementation of licensee security training programs and allow for increased flexibility, while maintaining safety and security. The requirements that were retained or modified would continue to capture the programmatic areas that licensees must implement to provide the appropriate training for security personnel. Training methods that were previously described in requirements would generally be retained in guidance as one acceptable method of meeting the requirements. Licensees would be required to ensure that the personnel who implement the physical protection program have the appropriate knowledge, skills, and abilities to effectively perform their assigned duties and responsibilities to accomplish the performance objective of protecting public health and safety.

The removal of the prescriptive security equipment lists from appendix B to part 73 would allow licensees to select equipment that best meets their operational needs and integrate new technologies as appropriate. The removal would reduce the need for exemptions or license amendments.

The proposed rule would remove the prescriptive requirements for 40 hours of on-the-job training, and would instead use a performance-based approach that allows a licensee to determine the appropriate number of on-the-job training hours. Modern training methodologies, job-specific competencies, and improved instructional systems design processes enable licensees to tailor training more precisely to the knowledge, skills, and abilities needed for each role. Allowing flexibility in determining the number of on-the-job training hours gives licensees the ability to align training with actual task complexity, prior experience, and demonstrated proficiency, rather than relying on a uniform time-based metric. The regulations would continue to require that on-the-job

training is documented and attested by a qualified training instructor or a security supervisor. The licensee would verify that the implemented training approach provides personnel with the capability to effectively execute their responsibilities under the safeguards contingency plan

(h) Appendix C to Part 73

The changes proposed in appendix C to part 73 would remove the prescriptive periodicity associated with the review of safeguards contingency plans to provide licensee flexibility in these types of reviews.

(i) Expand regulatory flexibility

The proposed rule would expand the regulatory options for physical security for new applicants under parts 50 and 52. Specifically, applicants would be able to select the most appropriate physical security rule for their design and approach for licensing by complying with either § 73.55 or § 73.100, “Technology-inclusive requirements for physical protection of licensed activities at advanced nuclear plants against radiological sabotage,” which was developed for reactors licensed under part 53. The distinctions between § 73.55 and § 73.100 largely reflect the fact that the existing reactor fleet was built without accounting for security during the initial design phase. The proposed revisions to § 73.55 in this rule would address the current configuration of the operating fleet and, similar to § 73.100, provide increased flexibility to accommodate the wide range of current and future reactor technologies. Currently, applicants under part 53 have the option of complying with either § 73.55 or § 73.100 for physical security. Extending this flexibility to applicants under parts 50 and 52 would ensure that future applicants have appropriate physical security options for licensing when designing their physical protection programs under part 50, 52, or 53. This proposal would include revisions to §§ 50.34, 52.79, and 73.100 to reflect this expanded regulatory flexibility for future applicants.

(ii) Access Authorization

The NRC is proposing revisions to its access authorization requirements under §§ 73.55 and 73.56 to promote program efficiency by providing appropriate flexibilities to licensees and reducing unnecessary program burdens, while maintaining safety and security. The proposed revisions would also provide additional relief from requirements for those licensees and applicants who demonstrate that no achievable target sets exist in accordance with proposed § 73.55(f).

(a) Changes to the milestone for program implementation

The proposed rule includes a risk-informed change that would extend the implementation milestone for when a licensee or other entity must transition from its construction-phase security measures (employed through appropriate site procedures for the control of personnel, access controls, and pre-employment screening during the construction phase) to an operational access authorization program that meets all of the applicable requirements of § 73.56.

Under the existing regulations, § 73.56(a)(3) requires licensees to implement the requirements of § 73.56 before fuel is allowed onsite (in the protected area). The proposed rule would change the milestone for implementation of an access authorization program from before fuel is allowed onsite (i.e., into the protected area) to before initial fuel load into the reactor.

This proposed milestone change is based on recent operating experience from implementing phased subpart K FFD programs and pre-employment screening at power reactor construction sites. Specifically, the NRC issued an exemption to the licensee for Vogtle Electric Generating Plant, Units 3 and 4, to delay implementing the access authorization program requirements of § 73.56 until initial fuel load (86 FR 67734; November 29, 2021). The NRC has reassessed the risks presented during the construction of nuclear power reactors and has determined that the currently established milestone for transition to an operations-phase access authorization program is not commensurate with current risk insights. The risk associated with unirradiated fuel does

not increase when the fuel arrives onsite, because its engineered safety features, storage, and configuration have not changed since the fuel was in transit. (For transit and receipt onsite, physical protection requirements under § 73.67 are applied to protect the fuel.) Safety and security risks associated with unirradiated nuclear fuel only begin to increase once the process of loading the fuel into its operating configuration begins. The operational milestone “before initial fuel load into the reactor” therefore corresponds more closely to the start of NRC-licensed activities that could result in consequences adverse to public health and safety or the common defense and security than does the current milestone of receipt of nuclear fuel onsite.

(b) Revisions to reduce unnecessary burden and prescriptiveness

The proposed changes to access authorization program requirements would revise and/or eliminate program elements that have been identified as being unnecessarily costly or burdensome and not adding commensurate value to site safety or security. Requirements in § 73.56 would be revised to reflect insights gained from operating experience in the years since the requirements were last revised in the Power Reactor Security Requirements final rule in 2009 (74 FR 13970; March 27, 2009). These changes would promote efficiency and effectiveness for commercial nuclear power plant licensees and applicants, while adequately maintaining safety and security.

Proposed revisions to § 73.56(d)(3) would remove prescriptive requirements for the verification of true identity. Some approved methods for verifying true identity (e.g., validating a foreign national’s claimed non-immigration status using independent sources of reliable information) would be maintained in applicable guidance contained in Regulatory Guide (RG) 5.66, “Access Authorization Program for Nuclear Power Plants.” This change would provide appropriate flexibilities to licensees in implementing identity verification requirements, and the NRC would maintain reasonable assurance regarding the trustworthiness and reliability of personnel unescorted through continued reporting of access authorization information to the Federal Bureau of Investigation (FBI) Threat Screening Center.

Proposed revisions to § 73.56(i)(1)(v) would remove the requirement to perform a credit history re-evaluation as part of the process for determining the continued trustworthiness and reliability of individuals. Operating experience has shown that, although conducting a credit history evaluation at the time that unescorted access is initially authorized is important towards making an initial determination regarding an individual's trustworthiness and reliability, re-evaluations of credit history add little value. Potential concerns regarding continued trustworthiness and reliability are more effectively identified through the required criminal history update and through licensee behavioral observation programs.

(c) Adjustment to annual supervisory review

The proposed rule would adjust the requirements in § 73.56(i)(1)(iv) regarding supervisory review for personnel who are maintaining unescorted access. As proposed by the NRC, if an individual's supervisor were to interact with that individual with a frequency that allows the supervisor to form an informed and reasonable opinion regarding the individual's behavior, trustworthiness, and reliability, then the supervisor would not be required to conduct an annual supervisory review. Otherwise, the individual would be subject to an annual (within 365 calendar days) supervisory review conducted in accordance with the requirements of the licensee's or applicant's behavioral observation program. This proposed adjustment would reduce the unnecessary redundancy of annual reviews for cases where an individual is already subject to regular review by their supervisor, while still ensuring that individuals would undergo supervisor review in instances where contact is less frequent, ensuring that the objectives of the behavior observation program would be met.

(d) Relaxations for licensees who opt into a U.S. Government monitoring and notification program

The proposed rule would modernize program requirements by adjusting the frequency of certain requirements (e.g., criminal history records checks and vital area access list authorization) in a manner that provides additional burden relief to those

licensees who opt into a U.S. Government continuous monitoring and notification program—such as the FBI Record of Arrest and Prosecution Background (Rap Back) service—through a Memorandum of Understanding with the NRC.

The FBI Rap Back service is a subscription-based program that provides continuous, automated notifications of new criminal activity associated with individuals who have undergone a fingerprint-based background check. Enrolling in such a service can substantially reduce the need for a licensee to rely on repeated background checks to ensure the continued trustworthiness and reliability of personnel. The proposed rule would reflect these benefits by reducing the frequency of required checks for those licensees enrolled in such a program. This change would help enable licensees to modernize their programs and reduce unnecessary burden, while ensuring that security is adequately maintained through the use of appropriate alternative processes.

(e) Reductions to the frequency of audits and record-retention periods

The proposed rule would reduce the frequency of audits required under § 73.56(n), “Audits and corrective action,” by extending audit intervals from 12 months to 24 months for contractors or vendors, and from 24 months to 36 months for licensee and applicant programs. The proposed audit interval for contractors or vendors would be shorter than the interval for licensee and applicant programs because contractor and vendor activities operate outside licensees’ routine processes and are less easily observable by licensees. The proposed rule would also reduce the records retention period in § 73.56(o)(2) from 5 years to 3 years. These proposed changes would reduce costs and administrative burdens while enhancing overall efficiency. With these changes, there would still be reasonable assurance that security will continue to be adequately maintained because licensees would still be required to periodically review the effectiveness of their programs, and the NRC would maintain the ability to effectively oversee program effectiveness through its inspection and oversight of licensee performance.

(f) Alternative requirements for licensees who demonstrate no achievable target sets exist in accordance with § 73.55(f)

The proposed rule would provide relief from certain human reliability requirements for licensees and applicants who could demonstrate no achievable target sets exist in accordance with proposed § 73.55(f) and who would not credit any active measures (e.g., operator action, mitigative action, detection, assessment, armed response) in making that demonstration. Under the proposed rule, such licensees would implement a program that meets the alternative access authorization requirements of § 73.120, “Access authorization program for commercial nuclear plants,” which were originally developed to provide alternative requirements for facilities licensed under 10 CFR part 53 that meet the criteria outlined in § 73.100(a)(1)(i).

Under the requirements of § 73.120, eligible licensee facilities would be relieved from the requirements to perform psychological assessments and reassessments in § 73.56(e), “Psychological assessment,” and to establish a full training program for behavioral observation (i.e., initial and refresher training including knowledge checks) in § 73.56(f), “Behavioral observation.” Such licensees would have the option to provide minimal guidance to personnel on reporting questionable behavior, similar to the Department of Homeland Security’s “If you see something, say something” campaign or a commensurate corporate behavior awareness program. This relief would be commensurate with the lower security risk posed by potential human actions at these facilities.

(iii) Category I Physical Fitness and Performance Evaluation Programs

The proposed changes to § 73.46 would reduce burden on current and future licensees. The proposed changes for facilities licensed to possess or use a Category I quantity of SNM are in the areas of security training, specifically for drills, exercises, and physical fitness requirements. The proposed rule would reduce the required frequency of security training exercises from four to a maximum of three per year. On an annual basis, the licensee would need to ensure that each shift participates in at least two

tactical response drills, one of which would test the security response using the response force and a mock adversary team. Additionally, the licensee would need to conduct at least one force-on-force exercise annually and ensure that each shift that implements the safeguards contingency plan protective strategy participates in one force-on-force exercise every three years. Licensees would continue to ensure the effectiveness of their security programs, as security officers would maintain the knowledge, skills, and abilities necessary for contingency response activities through annual recurring training.

The proposed changes for security drills and exercises captured in 10 CFR 73.46(b)(9) and the physical fitness test captured in 10 CFR 73.46(b)(10) would be revised to align with the approach taken for power reactors. These changes are being proposed to decrease the burden in the implementation of licensee security training programs and to allow for increased flexibility, while maintaining safety and security.

These revisions would streamline the current requirements for security drills, exercises, and the physical fitness test to eliminate certain prescriptive requirements, which in some instances are no longer necessary for the implementation of the training program. Existing licensees that are in compliance with § 73.46 as of the effective date of the final rule, if this proposed change is made effective in a final rule, would also be in compliance with the proposed revisions to the regulations and would not be required to modify their current physical fitness and performance evaluation programs.

(iv) Category II and Category III Material Security

(a) Performance-based requirements

The NRC proposes to modify § 73.67(d) for physical protection for fixed site facilities for SNM of moderate strategic significance. This proposal would build on previous efforts to risk-inform physical security regulations by shifting from prescriptive to performance-based requirements that would increase flexibility for current and future licensees; reduce unnecessary burden on licensees; and, where appropriate, allow for alternatives. The proposed changes to § 73.67 would support the agency's mission to

enable the deployment of nuclear energy technologies (e.g., the use of high-assay low-enriched uranium fuel supporting new types of reactors).

This proposed rulemaking for Category II quantities of SNM would address regulatory gaps and create a standardized approach for physical security. This would provide a consistent set of requirements for new applicants that use this type of SNM. Additionally, these changes would support efficiencies in the NRC's licensing and oversight programs.

The existing security requirements for possession and use of Category II quantities of SNM were originally established in 1979. Since that time, the NRC and other governmental agencies completed several studies to evaluate the risk and consequences associated with the physical protection of SNM. These studies were performed following the terrorist events of September 11, 2001, in part to evaluate and address changes in the threat environment. These studies and changes in the threat environment identified new vulnerabilities and risks that were not addressed by the then-existing regulations.

Subsequently, the NRC issued orders containing additional security measures to fuel cycle facilities licensed to possess Categories I and III quantities of SNM. At the time these orders were issued, the only facilities licensed to possess a Category II quantity of SNM were non-power reactors. To address the threat at these non-power reactor facilities, in 2002 and 2003, the NRC issued confirmatory action letters documenting the implementation of compensatory measures. However, additional security measures specific to a Category II quantity of SNM were not developed.

The NRC proposes to modify requirements in § 73.67 for Category II quantities of SNM to be largely performance-based, only retaining the prescriptive requirements that would be expected for all licensees subject to the requirements of § 73.67(d). The proposed rule would allow greater flexibility for both material and potential reactor licensees who would utilize these requirements for physical protection. This would permit

licensees to adjust their security to better correspond to what is needed to ensure adequate physical protection.

The performance objectives in § 73.67(d)(1)(ii) and (iii) would require licensees to provide prompt detection for Category II quantities of SNM, instead of the early detection standard used in § 73.67(a)(2)(i) and (ii). Additional measures contained in § 73.67(d)(1) would provide requirements to store material in a controlled access area, mitigate and delay the bulk theft of special nuclear material, analyze and identify site-specific conditions that affect the protective strategy, provide defense in depth, coordinate the physical security plan with other onsite plans to avoid conflicts, and manage the potential for adverse effects on safety, security, and material control. These proposed changes would allow licensees possessing Category II quantities of SNM at a fixed site to implement protective strategies that are commensurate to the attractiveness of the material.

Proposed § 73.67(d)(2) would include performance requirements for the physical protection capabilities of detection, assessment, response, communication, and access authorization. Proposed § 73.67(d)(2)(xiii) would add requirements for compensatory measures. This addition would specify performance objectives for compensatory actions that should be taken when an item relied on for security is in a degraded condition. This addition would ensure the effectiveness of the physical protection system under abnormal operating conditions such as inclement weather and equipment malfunctions.

The NRC proposes to remove the current § 73.67(d)(3) and replace it with a new proposed § 73.67(d)(3). The proposed replacement § 73.67(d)(3) would allow the Commission to adjust physical security requirements—either adding or removing measures—based on the specific risk posed by the individual facility and site conditions to ensure adequate protection. The NRC is issuing draft Regulatory Guide (DG)-5088, “Physical Protection of Special Nuclear Material of Moderate or Low Strategic Significance,” proposed Revision 2 to RG 5.59, for public comment with this proposed rule to support implementation of the proposed requirements.

Proposed § 73.67(d)(4), “Alternative measures,” as revised, would provide a regulatory method for licensees who may wish to use different protective measures that are demonstrated to meet the performance objectives and requirements in § 73.67(a) and (b)(1).

Existing licensees that are in compliance with § 73.67 as of the effective date of the final rule, if this proposed change is made effective in a final rule, would be in compliance with the proposed revisions to the regulation and would not be required to modify their current physical protection programs. However, existing licensees would be able to voluntarily adopt certain performance-based alternatives, which would allow for greater flexibility in implementing the requirements of § 73.67.

Licensees that would elect to implement the proposed revised performance objective would be required by proposed § 73.67(d)(1)(vi), (viii), (ix), and (x) to perform an analysis to identify the necessary plant equipment, mitigative measures, detection capabilities, assessment processes, and response needed to ensure the site’s physical protection program would be designed to prevent theft and diversion of SNM.

Alternatively, licensees that would elect to retain their existing physical protection programs to protect against theft and diversion of special nuclear material would be in compliance with the proposed performance objectives. All current licensees approved to possess a Category II quantity of SNM have approved security plans that include site-specific, performance-based security requirements that meet the proposed performance objectives, so an analysis of the proposed performance objectives would not be required. These licensees would continue to meet and implement the current requirements as relates to site-specific analysis for their physical protection program.

Licensees that would retain their current physical protection program would be able to elect to change their security plans and implementing procedures to reference the new proposed regulatory requirements using the existing § 70.32(e) process.

(b) Protection of Category II and Category III special nuclear material

The proposed rule would address an identified regulatory gap in the security requirements in § 73.67 for the protection of Category II and Category III special nuclear material among power reactor license holders. Paragraphs 73.67(d) and (f) would be modified to include an exception for part 52 licensees who will use Category II quantities of SNM inside a protected area. This change would align with Commission direction in SRM-SECY-22-0052, "Staff Requirements—SECY-22-0052—Proposed Rule: Alignment of Licensing Processes and Lessons Learned from New Reactor Licensing (RIN 3150-AI66)," dated November 20, 2024, to make security requirements for Category II and III quantities of special nuclear material brought on site at nuclear power reactors for new and existing facilities licensed under part 50 consistent with those requirements for facilities licensed under part 52. Under the current regulations, a part 50 licensee is exempt from the regulations, but a part 52 licensee is not. By providing this exemption for part 52 licensees, the proposed rule eliminates the need for part 52 licensees to comply with both § 73.67 and the more stringent § 73.55 requirements when the material is located inside a protected area. The § 73.55 requirements are designed to protect irradiated fuel from sabotage events at nuclear power reactors. Given the relative risks of irradiated and unirradiated fuel, it is acceptable to protect unirradiated reactor fuel and other nonfuel SNM brought onsite at a nuclear power reactor in accordance with § 73.67 until that material is protected in accordance with § 73.55. The change in this proposed rulemaking would reduce unnecessary regulatory burden and provide consistency between parts 50 and 52 applicants by providing the same exception for part 52 licensees. This proposed change is discussed further in Section VIII, "Backfitting and Issue Finality," in this document.

(v) Electronic Processing of Safeguards Information

Sections 73.22 and 73.23 currently restrict licensees to transmitting SGI using NRC-approved technology and storage on standalone computers, transmitting SGI for voice communications using only technology approved by the NRC, and processing

documents only on a standalone computer. Historically, the NRC has expected SGI to be treated more like classified information. These current regulations are very restrictive and not consistent with the threat environment, SGI's status as sensitive unclassified information, and the design basis threat's focus on threats posed by non-state actors.

The NRC is proposing to revise its regulations for the protection of SGI in §§ 73.22 and 73.23 to expand the means through which SGI can be transmitted for voice communications and to provide an option through which SGI can be viewed on networked computer systems. Sections 73.22(f)(3) and 73.23(f)(3) would be revised to allow an individual to transmit SGI for voice communications using commercially available digital technology that uses encryption algorithms that are compliant with or validated against an active and approved version of Federal Information Processing Standard (FIPS) 140. Additionally, the proposed rule would expand the ability to process SGI on computer systems. Currently, SGI may be stored on only standalone computers. The proposed rule would provide an option in § 73.22(g)(2) to store and process SGI on computer systems that permit viewing of the information on networked computers, using a virtual desktop or thin client architecture, provided that the systems storing the SGI would implement security controls that ensure the information is protected against unauthorized disclosure.

(a) Voice communications

The proposed rule would expand the means through which SGI could be transmitted for voice communications. The proposed changes in § 73.22(f)(3) would enable licensees to communicate SGI by voice using encryption algorithms that have been approved by the National Institute of Standards and Technology (NIST), rather than also requiring that they be submitted to the NRC for review and approval. Draft guidance changes would discuss appropriate measures to protect against spills (e.g., disabling transcription and recording, use in an area where only SGI authorized personnel are present, etc.).

Current § 73.23(f)(3) requires that SGI be transmitted only by NRC-approved secure electronic devices, encrypted by a method (FIPS 140-2 or later) approved by the NRC. Under the proposed § 73.23(f)(3), SGI would be transmitted only using a commercially available encryption system compliant with an active, approved version of FIPS 140. This change would eliminate the requirement for entities to seek NRC approval prior to using an encryption system, as long as it meets the FIPS 140 standard.

(b) Viewing safeguards information on networked computer systems

The proposed rule would provide an option through which SGI could be viewed on networked computer systems. Processing SGI on standalone computers creates a significant burden, particularly for new reactor vendors incorporating security by design principles. Additionally, the cybersecurity field has matured significantly since the SGI regulations were last modified. The proposed changes in § 73.22(g)(2) would give licensees the option to use networked systems that would implement security controls specified by NIST as being appropriate for controlled unclassified information (NIST SP 800-171) using a thin client or virtual desktop architecture that would protect SGI from unauthorized disclosure and from being transmitted or stored on unapproved computers.

(vi) Decommissioning

As discussed in Section IV.B.(i), “Security Requirements for ISFSIs Located Outside a Reactor’s Protected Area,” of this document, this proposed rule would streamline and expedite the reduction of resources needed to implement the physical protection program as a site in decommissioning transitions from storing fuel in the spent fuel pool to dry storage. Those proposed changes are consistent with the draft amendments presented to the Commission in SECY-24-0011.

(vii) Addressing Issues Related to the 2023 Enhanced Weapons Final Rule

This proposed rule would revise part 73 definitions, physical security event notification requirements, and suspicious activity reporting requirements to resolve industry concerns and challenges from the 2023 Enhanced Weapons final rule (88 FR 15864; March 14, 2023).

The proposed amendments would modify requirements issued in the 2023 Enhanced Weapons final rule that posed concerns and challenges for industry to effectively and efficiently implement. Industry identified these concerns and challenges to the NRC and requested exemptions from these requirements (e.g., definitions of specific terms, protocols for contacting local Federal Aviation Administration (FAA) control towers, and the timelines associated with certain notifications). The NRC proposes to clarify or remove other provisions from the 2023 Enhanced Weapons final rule that were identified as imposing unnecessary burdens. The NRC was able to address many of the implementation issues by revising three RGs in 2024 (i.e., RG 5.62, Revision 3, “Physical Security Event Notifications, Reports, and Records”; RG 5.86, Revision 1, “Preemption Authority, Enhanced Weapons Authority, and Firearms Background Checks”; and RG 5.87, Revision 1, “Suspicious Activity Reports Under 10 CFR Part 73”). Other issues that could be resolved only by rulemaking were discussed in a public meeting on July 31, 2025 (“Summary of July 31, 2025, Meeting with External Stakeholders Discussing Perspectives on Recent Security Event Notifications,” dated December 18, 2025). The proposed changes to §§ 73.2, “Definitions,” 73.1200, “Notification of security events,” 73.1205, “Written follow-up reports of security events,” 73.1210, “Recordkeeping of security events,” and 73.1215, “Suspicious activity reports,” in this proposed rule would resolve these issues and are reflected in the proposed revisions to supporting guidance in DG-5089 and DG-5098.

Section 73.1200 would be revised in several locations to increase consistency between facility-based and transportation-based event notifications (e.g., use of hostile action versus hostile threat, adding notification of thefts of spent nuclear fuel or high-level radioactive waste from facilities). The NRC proposes to clarify language on the elimination of duplication to reduce burden for a single event that had both a physical security component (under part 73) and an information security component (under part 95).

Sections 73.1205 and 73.1210 would be revised to correct unnecessary records retention requirements by replacing the phrase “whichever is later” (which implied an obligation after license termination) with “whichever is earlier.” Section 73.1205 would also be revised to remove the requirement for written follow-up reports subsequent to 15-minute and 8-hour event notifications to reduce industry burden. For events of high security significance requiring notification within 15 minutes (i.e., actual or expected attacks on a facility or shipment), prompt onsite follow-up by the NRC would occur and would be documented sufficiently by the NRC and the licensee to obviate the need for a licensee’s written follow-up report within 60 days. For events of low security significance requiring notification within 8 hours, documented follow-up can occur during the NRC’s next routine security inspection.

The NRC would make conforming changes to NRC Form 366, “Licensee Event Reports,” to remove references to § 73.77, “Cybersecurity event notifications,” which would be revised by this rulemaking as discussed in Section IV.C.(x).

Section 73.1215 would be revised to use more generic language for suspicious activity reports to the FAA. Specifically, references to “aircraft” would be revised to “crewed/uncrewed aviation-related assets” and the term “local FAA control tower” would be revised to “applicable FAA facility.” The revised language would provide greater flexibility in implementing the reporting provisions and making these reports while meeting FAA operational (workload and airspace) considerations. The NRC proposes to add language on the elimination of duplication to address suspicious activity reports that would otherwise be required under both § 73.1215 and § 37.57, “Reporting of events” (e.g., a licensee storing both spent fuel and greater than class C waste at an ISFSI).

(viii) Personnel Identification System

Section 73.70, “Records,” would be revised to add a conforming change to reflect the proposal in § 73.55(g)(6)(ii) to allow licensees to use a personnel identification system, rather than specifically requiring numbered badges. With this change, licensees would have an option for the method of compliance for logging individuals that have

been issued identification to enter a protected area. This proposed change could also reduce the cost of providing access to individuals that have access to a protected area.

Under the current § 73.70, certain licensees are required to maintain records of the names, addresses, and badge numbers of all individuals authorized to have access to vital equipment or special nuclear material, and the vital areas and material access areas to which authorization is granted. This proposed change would require licensees who elect to use an alternative personnel identification system to retain the records for individuals enrolled in that system. By adding this option, power reactor licensees would have an option for complying that also reduces the cost of producing badges for personnel that have access to vital areas or special nuclear material.

(ix) Definitions

Section 73.2 would be updated to reflect various regulatory changes in 10 CFR part 73 that affect multiple categories of licensees by revising the definitions of “Physical barrier,” and “Contraband.” A new definition for “Target set” would be added. As it relates to the relevant sections, these proposed changes would enhance clarity and promote consistency.

The definition for “Physical barrier” would be revised to allow for increased flexibility in licensee methods for meeting part 73 requirements. This change would reduce the need for licensees to submit licensing actions to modify their physical barriers in ways that depart from the current, prescriptive requirements. Instead, licensees could adopt a performance-based approach based on the function of the barrier in the physical protection program.

The definition of “Contraband” would be revised to remove reference to “disease causing agents” because the ability to identify these agents would exceed the reasonable capabilities of a licensee’s physical protection program. With the removal of “disease causing agents,” the term “dangerous materials” would be redundant to the existing terms in the definition of contraband and therefore would also be removed. Separately, language in the definition of contraband regarding electronic devices would

be removed. The existing requirements in 10 CFR part 95, “Facility Security Clearance and Safeguarding National Security Information and Restricted Data,” and 32 CFR part 117, “National Industrial Security Program Operating Manual (NISPOM),” are sufficient to protect classified information from unauthorized electronic devices, which pose an information security concern rather than a physical security concern.

A definition for “Target set” would be added in § 73.2. This term was previously defined in regulatory guidance, including RG 5.81, Revision 1, “Target Set Identification and Development for Nuclear Power Reactors,”[2] and NUREG-2203, “Glossary of Security Terms for Nuclear Power Reactors.” The NRC proposes to revise that definition to reflect the dose consequence performance objective of proposed § 73.55.

(x) Cybersecurity

(a) Regulatory guidance revisions

The existing regulatory framework for cybersecurity under § 73.54 is performance based and provides reasonable assurance that digital computer and communication systems and networks associated with safety, security, and emergency preparedness (SSEP) functions are adequately protected against cyberattacks up to and including the design basis threat, as defined in § 73.1. Commercial nuclear power plant licensees can choose from approved guidance documents (e.g., RG 5.71, “Cybersecurity Programs for Nuclear Power Reactors,” and NEI 08-09, “Cyber Security Plan for Nuclear Power Reactors”) for well-established standardized approaches to meet the cybersecurity requirements in § 73.54.

The NRC is proposing to update RG 5.71 to reflect lessons learned from operating experience while ensuring that licensees continue to maintain reasonable assurance of safety and security. The proposed RG 5.71 updates would effectively result in reducing regulatory burden by, for example, focusing on safety and security over general cybersecurity hygiene—cutting approximately 19 percent of controls—and

---

[2] Revision 1 to RG 5.81 contains Official Use Only—Security Related Information. Therefore, this RG is withheld from public disclosure but is available to those affected licensees, stakeholders who have established a need to know, and cleared stakeholders who have access authorization.

allowing licensees to take credit for cybersecurity best practices already in use (beyond those specified in RG 5.71).

(b) Event notifications

The requirements for commercial nuclear power plant licensees to notify the NRC of certain cybersecurity-related events that adversely impact or could have impacted SSEP functions are defined in § 73.77, with supporting guidance in RG 5.83, “Cybersecurity Event Notifications.” To date, no licensee has made a notification under these provisions. In lieu of reporting incidents in accordance with the requirements of § 73.77, licensees have used the existing notification processes under §§ 50.72 and 50.73 (for safety-related events) and § 73.1200 (for security-related events). This proposal would simplify the regulation in § 73.77 by eliminating specific event notifications and instead redirect licensees to the aforementioned notification processes (i.e., a cybersecurity-related event notification would use these safety-related or security-related regulations, based upon the affected function). This approach would allow the NRC to withdraw RG 5.83 and incorporate cybersecurity-related events reporting into the broader, established notification processes under parts 50, 53, and 73.

(c) Expand regulatory flexibility

To support innovation and modernization of the existing cybersecurity regulatory framework, this proposed rule would expand the regulatory options for new applicants under parts 50 and 52. Specifically, applicants would be able to select the most appropriate cybersecurity rule for their design and risk profile by complying with either § 73.54 or § 73.110, “Technology-inclusive requirements for protection of digital computer and communication systems and networks,” which was developed for part 53. Differences between the § 73.54 requirements and those in § 73.110 are primarily based on the implementation of a consequence-based approach to cybersecurity in § 73.110 that provides flexibility to accommodate the wide range of reactor technologies to be assessed by the NRC. A graded approach based on consequences would account for the differing risk levels among reactor technologies.

This proposal would include revisions to §§ 73.54, 73.55, 73.77, and 73.110; the companion regulatory guidance for § 73.110, DG-5103 (proposed Revision 1 to RG 5.96), “Establishing Risk-Informed and Technology-Inclusive Cybersecurity Programs for Commercial Nuclear Plants”; and §§ 50.34 and 52.79 to reflect this expanded regulatory flexibility.

This proposal would eliminate the existing introductory paragraph of § 73.54. That statement was originally intended to require that operating nuclear power plants, at the time of rule implementation in 2009, establish, implement, and maintain a cybersecurity program. All currently operating nuclear power plants have fully implemented their cybersecurity plans and will continue to maintain their plans per the requirements of § 73.55 and § 73.54.

The NRC is also proposing revisions to § 73.54(g) as conforming changes to align with the expansion of regulatory options for new applicants. Specifically, the cybersecurity program review requirement would be independent of the physical security program.

(xi) Design Requirements

The NRC is proposing amendments to § 50.34(a)(3)(i) and § 52.79(a)(4)(i) to require that safety and security be considered together in the design process such that, where possible, security issues are effectively resolved through design and engineered security features. This approach, which is consistent with the requirement in § 53.440(f), ensures consideration is given to safety and security together throughout the plant’s lifetime, including the design process and prior to implementing changes to plant configurations, to ensure risks are effectively managed. This evaluation helps determine whether enhancements to the design basis or physical protection system are warranted. Incorporating security strategies and design features early in the design process can be significantly more efficient and cost-effective than retrofitting these measures after the plant has been designed or constructed.

D. Facility Security Clearance and Safeguarding of National Security Information and Restricted Data (Part 95)

The proposed rule would revise 10 CFR part 95 to remove requirements that are duplicative and ensure alignment with 32 CFR part 117 by providing references to 32 CFR part 117 where appropriate. Furthermore, specific NRC prescriptive requirements would be eliminated to resolve any conflicting regulations.

Part 95 establishes requirements for licensees, applicants, and other entities that obtain a facility security clearance from the NRC, as well as the requirements for the protection of classified matter. These requirements are based on the National Industrial Security Program Operating Manual (NISPOM), which was codified in regulation in February 2021, at 32 CFR part 117. Part 95 ensures that entities that fall under NRC cognizance meet the requirements of the NISPOM.

The regulations in 32 CFR part 117 establish the NRC as the cognizant security agency for NRC-cleared entities that are issued facility security clearances. Currently, cleared entities under NRC cognizance are subject to both 10 CFR part 95 and 32 CFR part 117, which has resulted in the establishment of duplicative and inconsistent regulatory requirements for cleared entities.

Under this proposed rule, the NRC would revise 10 CFR part 95. The proposed changes would not affect any existing regulatory guidance, but inspection procedures related to part 95 would be updated. The NRC would remove requirements from 10 CFR part 95 that are duplicative or inconsistent with the requirements in 32 CFR part 117. Part 95 would retain only those requirements and processes that are unique to NRC-cleared entities.

Section 95.1, “Purpose,” would be revised to identify that the purpose of part 95 is to implement the National Industrial Security Program, as described in 32 CFR part 117.

Section 95.5 would be revised to remove unused definitions or those definitions that are duplicative to definitions in 32 CFR part 117.

Section 95.11, “Specific exemptions,” would be revised to change the section title to “Specific exemptions and waivers,” to include reference to the NRC’s ability to issue waivers in accordance with 32 CFR part 117.

Section 95.17, “Processing facility clearance,” would be renamed “Facility clearance process” for clarity. Requirements unrelated to the facility clearance process that had previously been in § 95.17 were moved to other more relevant sections. Other revisions would clarify that the review referred to in § 95.17 is an operational readiness review (rather than a security review). The NRC would revise § 95.17 to use the definition of “key management personnel” found in 32 CFR part 117.

The NRC proposes to delete §§ 95.18, “Key personnel”; 95.25, “Protection of National Security Information and Restricted Data in storage”; 95.27, “Protection while in use”; 95.29, “Establishment of Restricted or Closed areas”; 95.31, “Protective personnel”; 95.35, “Access to matter classified as National Security Information and Restricted Data”; 95.45, “Changes in classification”; and 95.51, “Retrieval of classified matter following suspension or revocation of access authorization,” because they duplicate provisions in 32 CFR part 117.

Section 95.19, “Changes to security practices and procedures,” would be revised to remove the requirement to resubmit the Standard Practice Procedures Plan every 5 years. This change would result in a reduction in licensee burden.

The NRC proposes to add § 95.24, “Safeguarding National Security Information and Restricted Data,” which would be a new section. This section would retain existing requirements from 95.25, “Protection of National Security Information and Restricted Data in storage,” related to the maintenance of keys and padlocks used to protect classified information. There would be no additional licensee burden associated with this change.

Sections 95.33, “Security education,” 95.34, “Control of visitors,” 95.37, “Classification and preparation of documents,” 95.39, “External transmission of documents and material,” 95.43, “Authority to reproduce,” and 95.47, “Destruction of

matter containing classified information," would be modified to remove specific requirements and instead require that cleared entities conduct these activities in accordance with 32 CFR part 117.

Section 95.49, "Security of automatic data processing (ADP) systems," would be renamed "Authorization to operate national security systems," consistent with usage in 32 CFR part 117. Specific requirements would be deleted, and the revised section would require cleared entities to process classified information on information technology or operational technology systems in accordance with 32 CFR part 117.

The NRC would revise § 95.57, "Reports," to establish reporting requirements consistent with the provisions in 32 CFR part 117 that state that the cognizant security agency (CSA) (in this case, the NRC) will provide guidance on reporting security events. The proposed revision would provide that all actual or suspected losses or compromises of classified information would be reported to the NRC Headquarters Operations Center within one hour of discovery, with a written follow-up submitted within 48 hours. If it is determined that no loss, compromise, or suspected compromise occurred, a written report documenting this determination would be submitted in accordance with § 95.9, "Communications," within 48 hours of reaching that conclusion. If the NRC is not the CSA, the entity would first report to their applicable CSA and then to the NRC. This revision would also eliminate the previous requirement for monthly logs.

V. Specific Requests for Comments

The NRC is seeking advice and recommendations from the public on the proposed rule. The NRC is particularly interested in comments with supporting rationales from the public on the following questions. In addition to the general discussion in Section IV, additional context is provided for certain questions in order to help the public comment on these issues.

Requirements for Vital Areas

Part 73 establishes requirements for the physical protection of licensed activities and facilities, which includes nuclear power reactors and Category I facilities. Section 73.2 defines vital areas and vital area equipment. The vital area concept focuses protective measures and access controls on locations housing equipment and functions essential to preventing significant radiological consequences from malevolent acts.

The licensees and the NRC have gained additional experience implementing the requirements associated with vital areas. The current approach for power reactors to protect their facilities focuses on the use of target sets (plant equipment and operator actions) that may or may not involve vital equipment. Evolving plant design changes, digital modernization, and operational practices may warrant an assessment of whether the vital area concept remains optimally defined and implemented across 10 CFR part 73 are clear, efficient, and risk-informed.

Question 1: The NRC seeks stakeholder input on whether to revise or remove the term “vital areas” for power reactor facilities. Please explain the basis for your response.

Performance Objective

Under current part 73, licensees subject to § 73.55 must meet the performance objective in § 73.55(b)(3) of protecting against significant core damage and spent fuel sabotage. The NRC is proposing to change the performance objective from protecting against significant core damage and spent fuel sabotage to a broader goal of preventing release of radionuclides from any source that exceeds the dose reference values defined in § 50.34(a)(1)(ii)(D)(*1*) and (*2*), § 52.79(a)(1)(vi)(A) and (B), or § 53.210, as applicable, given that the term “core damage” is not necessarily applicable for some reactor technologies and designs.

Question 2: The NRC seeks stakeholder input on the following:

a. How would this change impact the security programs of current licensees?

b. Would changing the performance objective in § 73.55(b)(3) provide any benefit to future licensees given that § 73.100 already offers a flexible, technology-inclusive performance objective for new reactors?

Fitness-for-Duty Program Requirements

Part 26 establishes requirements for FFD programs at NRC-licensed facilities. These requirements have been developed over time to provide, in part, a level of detail needed to support licensee legal considerations (e.g., related to donor protections, the accuracy and reliability of tests performed, and the defensibility of licensee decisions regarding sanctions imposed on individuals because of FFD program violations). The proposed rule includes several changes to 10 CFR Part 26 intended to reduce regulatory burden while increasing program effectiveness, efficiency, and flexibility.

Question 3: Are there additional changes that the NRC should consider to streamline or simplify FFD program requirements for NRC licensees? For example, are there specific requirements in 10 CFR Part 26 or other related regulations that could be transitioned to regulatory guidance (e.g., to reduce prescriptiveness and allow licensees and applicants to propose alternate methodologies in their licensing applications)? Please explain the basis for your response and provide specific recommendations to the extent possible.

Applicability of Changes to New Reactor Licensees and Applicants

The proposed rule includes several changes to prescriptive security and fitness-for-duty requirements that are based on the operating experience and performance history of the operating reactor fleet. Examples of such changes for power reactors include the proposed reduction in the number of required tactical response drills and force-on-force exercises, elimination of the annual reports of waivers and fatigue management program information, and reduction in annual random testing rate for employees that do not perform critical safety- or security-related activities. New reactor

licensees and applicants, however, may lack similar operating experience and performance history in these areas.

Question 4: Should the proposed changes to prescriptive security and fitness-for-duty requirements that are based on the operating experience and performance history of the operating reactor fleet be applicable to all licensees and applicants, as currently proposed, or should the NRC develop criteria to limit the applicability of these proposed changes? If the NRC should develop criteria to limit the applicability of these proposed changes, what criteria should the NRC consider? Please provide a basis for your response.

VI. Regulatory Flexibility Certification

As required by the Regulatory Flexibility Act of 1980, 5 U.S.C. 605(b), the Commission certifies that this rule, if adopted, will not have a significant economic impact on a substantial number of small entities. This proposed rule affects only the licensing and operation of nuclear power plants. The companies that own these plants do not fall within the scope of the definition of “small entities” set forth in the Regulatory Flexibility Act or the size standards established by the NRC (10 CFR 2.810).

VII. Regulatory Analysis

The NRC has prepared a draft regulatory analysis on this proposed regulation. The analysis examines the costs and benefits of the alternatives considered by the NRC. The NRC requests public comment on the draft regulatory analysis. The regulatory analysis is available as indicated in the “Availability of Documents” section of this document. Comments on the draft analysis may be submitted to the NRC as indicated under the ADDRESSES caption of this document. As discussed in Section IV.A.(i)(k) of this document, the NRC also requests public input on the costs and benefits of subpart F of 10 CFR part 26.

VIII. Backfitting and Issue Finality

The Commission has completed a backfitting and issue finality assessment for this proposed rule under §§ 50.109, “Backfitting”; 53.1590, “Backfitting”; 70.76, “Backfitting”; and 72.62, “Backfitting,” and the issue finality provisions of part 52 and part 53. Also, a number of the changes in this proposed rule would not be subject to the backfitting and issue finality requirements. This assessment is available as indicated in the “Availability of Documents” section of this document.

One set of changes in this proposed rule would constitute backfitting, as that term is defined in § 50.109 and described in NRC Management Directive 8.4, “Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests.” The proposed changes to §§ 73.67(d) and 73.67(f) to clarify the appropriate security requirements for Category II and III quantities of SNM stored within the owner-controlled area but outside the protected area at 10 CFR part 50 nuclear power reactors could impose a change to those licensees’ required physical security programs, thereby meeting the definition of “backfitting” in § 50.109(a)(1). As described in the backfitting assessment, these proposed backfits would be justified on the basis that the proposed changes would be necessary to ensure that these facilities provide adequate protection to the health and safety of the public and are in accord with the common defense and security.

The NRC is issuing fifteen DGs that, if finalized, would provide guidance on the methods acceptable to the NRC for complying with aspects of this proposed rule. As discussed in the DGs, applicants and licensees would not be required to comply with the positions set forth in the DGs. Therefore, issuance of the DGs in final form would not constitute backfitting or forward fitting, as that term is defined and described in Management Directive 8.4, or affect the issue finality of any approval issued under part 52.

IX. Cumulative Effects of Regulation

The NRC seeks to minimize potential negative consequences resulting from the cumulative effects of regulation (CER). The NRC believes that the de-regulatory impacts of this rulemaking activity are unlikely to cause implementation challenges for stakeholders. In addition, during the pendency of this rulemaking, the NRC is deprioritizing issuance of regulatory actions that might influence the implementation date for the new rule requirements (e.g., orders, generic communications, license amendment requests, and inspection findings of a generic nature).

To fully understand any potential CER implications that could result from this rulemaking, the NRC is asking the following questions. Response to these questions is voluntary and any input will be considered during development of the final rule.

1. The NRC is proposing an effective date that will be 30 days after the date of publication of a final rule. The NRC is proposing a compliance (implementation) date that will be 180 days after the date of publication of the final rule. Does this provide sufficient time to implement the proposed requirements and associated guidance? Please provide a rationale for your response.

2. Are there unintended consequences related to this rulemaking and how should they be addressed? Please provide a rationale for your response.

3. Please comment on the NRC's cost and benefit estimates in the regulatory analysis that supports this proposed rule.

X. Plain Writing

The Plain Writing Act of 2010 (Pub. L. 111-274) requires Federal agencies to write documents in a clear, concise, and well-organized manner. The NRC has written this document to be consistent with the Plain Writing Act as well as the Presidential Memorandum, "Plain Language in Government Writing," published June 10, 1998 (63 FR 31885). The NRC requests comment on this document with respect to the clarity and effectiveness of the language used.

XI. National Environmental Policy Act

The Commission has determined under the National Environmental Policy Act of 1969, as amended, and the Commission's regulations in subpart A, "National Environmental Policy Act—Regulations Implementing Section 102(2)," of part 51, "Environmental Protection Regulations for Domestic Licensing and Related Regulatory Functions," that this proposed rule, if adopted, would not be a major Federal action significantly affecting the quality of the human environment, and an environmental impact statement would not be required, because implementation of the proposed rule requirements would not have a significant environmental effect. The proposed rulemaking would amend requirements that are administrative in application, are matters of procedure, or provide an equivalent level of safety as existing requirements. Therefore, the environmental impacts from the implementation of this proposed rule would be similar to those occurring under existing requirements.

The preliminary determination of the Commission's environmental assessment and finding of no significant impact is that there would be no significant effect on the quality of the human environment from this rulemaking action. Comments on any aspect of this environmental assessment and finding of no significant impact may be submitted to the NRC as indicated under the ADDRESSES section of this document. The environmental assessment is available as indicated under the "Availability of Documents" section of this document. This environmental assessment and proposed finding of no significant impact can be tracked with identification number NEPA ID EAXX-429-00-000-1771377270. The Commission will consider timely public comments received on the environmental assessment and draft finding of no significant impact in determining whether to issue a final finding of no significant impact for the final rule.

XII. Paperwork Reduction Act

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

Type of submission: New

The title of the information collection: Modernizing Security Requirements

OMB approval numbers: 3150-0002, 3150-0009, 3150-0011, 3150-0047, 3150-0104, 3150-0132, 3150-0146, and 3150-0151.

The form number if applicable: NRC Forms 366, 891, and 892

How often the collection is required or requested: Initial submission of revised security or cybersecurity plans in response to regulatory changes are one-time requirements. Notifications and written reports of physical security events, fitness-for-duty policy violations, or suspicious activity, are submitted on occasion and must be submitted promptly after the event occurs (e.g., within 15 minutes, 1 hour, 4 hours, 8 hours, or 24 hours, depending on the event's significance). Certain collections are required on a quarterly basis, such as the submission of blind performance test samples to HHS-certified laboratories for drug and alcohol testing program oversight. Annual requirements include the collection and reporting of fitness-for-duty program performance data to the NRC. Retention periods for records under the proposed rule vary depending on the type of information collected, from two to three years, until the completion of all related legal proceedings, or until license termination.

Who will be required or asked to respond: Existing and future applicants and licensees under 10 CFR Parts 50, 52, and 53.

An estimate of the number of annual responses: 10 CFR Part 26: -26,077 (-167 reporting responses + -46 recordkeepers + -25,864 third party disclosure responses); 10 CFR Part 50: 3.6 (3.6 reporting responses + 0 recordkeepers + 0 third party disclosure responses); 10 CFR Part 52: 1 (1 reporting responses + 0 recordkeepers + 0 third party disclosure responses); 10 CFR Part 70: 0.3 (0.3 reporting responses + 0 recordkeepers + 0 third party disclosure responses); 10 CFR Part 73: -52 (-2 reporting responses + -56 recordkeepers + 6 third party disclosure responses); 10 CFR Part 95: -20 (0 reporting responses + -20 recordkeepers + 0 third party disclosure responses).

The estimated number of annual respondents: 10 CFR Part 26: 25,749 respondents; 10 CFR Part 50: 3.6 respondents; 10 CFR Part 52: 1 respondent; 10 CFR Part 70: 0.3 respondents; 10 CFR Part 73: 56 respondents; 10 CFR Part 95: 20 respondents.

An estimate of the total number of hours needed annually to comply with the information collection requirement or request: 10 CFR Part 26: -42,271 (-1,092 reporting + -2,644 recordkeeping + -38,535 third party disclosure); 10 CFR Part 50: -788 (-788 reporting + 0 recordkeeping + 0 third party disclosure); 10 CFR Part 52: -250 (-250 reporting + 0 recordkeeping + 0 third party disclosure); 10 CFR Part 70: -75 (-75 reporting + 0 recordkeeping + 0 third party disclosure); 10 CFR Part 73: -25,636 (-1 reporting + -25,659 recordkeeping + 24 third party disclosure); 10 CFR Part 95: -2 (0 reporting -2 recordkeeping + 0 third party disclosure).

Abstract: The NRC is proposing to amend its regulations to reduce overly prescriptive requirements and modernize security and fitness-for-duty requirements to enhance efficiency and regulatory flexibility. This effort is consistent with, and implements, the

direction in E.O. 14300 which directs the NRC to conduct a comprehensive review and revision of its regulations. The proposed revisions are intended to reduce regulatory burden, where appropriate, while continuing to provide reasonable assurance that safety and security will be adequately maintained at NRC-licensed facilities. The proposed rule covers a wide range of topics, including the following areas that would result in new or revised changes in recordkeeping and reporting requirements:

- FFD Programs. The NRC is proposing effectiveness and efficiency improvements to the drug and alcohol testing and fatigue management requirements based on lessons learned from implementing 10 CFR Part 26, to align with select changes made by other Federal agency drug testing programs, and to address several petitions for rulemaking.
- Security Requirements for ISFSIs. The proposed rule would revise security requirements for ISFSIs to improve clarity and consistency between the requirements for general license ISFSIs and specific license ISFSIs.
- Physical Security Requirements. The NRC is proposing to modernize and streamline physical security requirements for nuclear power reactors and materials by shifting from prescriptive rules to performance-based, risk-informed criteria.
- Facility Security Clearance and Safeguarding of National Security Information and Restricted Data. The NRC is proposing to revise 10 CFR Part 95 to remove requirements that are duplicative and to ensure alignment with 32 CFR Part 117.

The proposed rule would impose burden associated with new optional information collections in NRC Form 891. NRC Form 366 would be updated to remove a regulatory reference. In addition, if paragraph 26.203(e) were deleted as proposed, the NRC would no longer need NRC Form 892.

The NRC is seeking public comment on the potential impact of the information collection(s) contained in this proposed rule and on the following issues:

1. Is the proposed information collection necessary for the proper performance of the functions of the NRC, including whether the information will have practical utility? Please explain your response.

2. Is the estimate of the burden of the proposed information collection accurate? Please explain your response.

3. Is there a way to enhance the quality, utility, and clarity of the information to be collected? Please explain your response.

4. How can the burden of the proposed information collection on respondents be minimized, including the use of automated collection techniques or other forms of information technology?

A copy of the OMB clearance package and proposed rule are available in the "Availability of Documents" section of this document may be viewed free of charge by contacting the NRC's Public Document Room reference staff at 1-800-397-4209, at 301-415-4737, or by email to PDR.Resource@nrc.gov. You may obtain information and comment on submissions related to the OMB clearance package by searching on https://www.regulations.gov under Docket ID NRC-2025-1303.

You may submit comments on any aspect of these proposed information collections, including suggestions for reducing the burden and on the above issues, by the following method:

Federal rulemaking website: Go to https://www.regulations.gov and search for Docket ID NRC-2025-1303.

Submit comments by **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]**. Comments received after this date will be considered if it is practical to do so, but the NRC staff is able to ensure consideration only for comments received on or before this date.

Public Protection Notification

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

XIII. Executive Orders

The following are Executive orders that are related to this proposed rule:

A. Executive Order 12866: Regulatory Planning and Review (As Amended by Executive Order 14215, Ensuring Accountability for All Agencies)

The Office of Information and Regulatory Affairs (OIRA) has determined that this proposed rule is a significant regulatory action under section 3(f) of E.O. 12866, though not economically significant under section 3(f)(1). Accordingly, the NRC submitted this proposed rule to OIRA for review. The NRC is required to conduct an economic analysis in accordance with section 6(a)(3)(B) of E.O. 12866. More can be found in Section VII of this document, “Regulatory Analysis.”

B. Executive Order 14154: Unleashing American Energy

The NRC has examined this proposed rule and has determined that it is consistent with the policies and directives outlined in E.O. 14154.

C. Executive Order 14192: Unleashing Prosperity Through Deregulation

This action is tentatively determined to be a deregulatory action as defined by E.O. 14192. The NRC estimates that this rule generates $45.2 million in annualized costs savings at a 7 percent discount rate, discounted relative to year 2024, over a perpetual time horizon. Details on the estimated costs of this proposed rule can be found in Section VII of this document.

D. Executive Order 14267: Reducing Anti-Competitive Regulatory Barriers

E.O. 14267 requires the NRC to identify anti-competitive regulations for rescission or modification. The NRC identified several such changes in 10 CFR part 26. The proposed rescission/modification of the regulations supports the objectives of E.O.

14267 by removing regulatory requirements that could create unnecessary barriers to entry for new market entrants.

First, by expanding the acceptable credentials to serve as an SAE to include licensed marriage and family therapists, the proposed rule would allow licensees to consider additional candidates to potentially serve as SAEs. Second, by revising the medical degree requirements for MROs to include medical degrees obtained in foreign countries that are equivalent to a Doctor of Medicine or Doctor of Osteopathy degree obtained in the United States, the proposed rule would expand the potential pool of candidates available to provide MRO services. Finally, proposed changes to the blind performance testing programs would include the removal of the requirement for licensees to submit additional blind performance test samples in the initial 90 days of testing with a new HHS-certified laboratory. This change would enhance competitiveness for new market entrants by removing a potential disincentivizing factor for a licensee that may want to change to another HHS-certified laboratory.

Additionally, the proposed rule would remove outdated provisions no longer in use by industry. These pertain to LTFs and reflect how the free market has driven changes in the drug testing programs under 10 CFR part 26. At the inception of 10 CFR part 26 FFD programs in 1990, many licensees utilized LTFs at their sites to perform initial drug testing. Over time, the advantages of LTF testing decreased as the performance and capabilities at HHS-certified laboratories (price-competitive, private, and for-profit entities), significantly improved. LTFs have not been a viable testing option for licensees because of the increasing sophistication and complexity of drug testing (e.g., substances, biological specimens) and the financial burden associated with staffing, equipping, and maintaining these facilities. Furthermore, removal of LTF provisions, along with the removal of barriers to licensees contracting with new laboratories as discussed in Section IV.A.(i)(c)1. of this document, would serve to further incentivize new market entrants by removing potential barriers to entry.

E. Executive Order 14270: Zero-Based Regulatory Budgeting to Unleash American Energy

E.O. 14270 requires the NRC to insert a conditional sunset date into all new or amended NRC regulations provided the regulations are (1) promulgated under the Atomic Energy Act of 1954, as amended (AEA), the Energy Reorganization Act of 1974, as amended (ERA), or the Nuclear Waste Policy Act of 1982, as amended (NWPA); (2) not statutorily required; and (3) not part of the NRC's permitting regime. The NRC determined that the regulatory changes proposed in this rule are part of the NRC's regulatory permitting scheme authorized by the AEA, ERA, or NWPA. Therefore, the NRC views this rulemaking to be outside the scope of E.O. 14270 and did not insert conditional sunset dates for the regulatory changes in this proposed rule.

XIV. 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 revise the NRC's requirements in 10 CFR parts 26, 72, 73, and 95 to modernize security and FFD programs by updating and clarifying regulatory provisions, streamlining administrative processes, and providing additional compliance flexibilities. These proposed changes are tailored to the unique safety and security needs of NRC licensees and would not create a broadly applicable technical standard suitable for adoption by voluntary consensus standards bodies. This action would not constitute the establishment of a standard that contains generally applicable requirements.

XV. Availability of Guidance

The NRC is issuing draft guidance for public comment, as described in this section, to support implementation of the proposed requirements in this rulemaking. The

draft guidance is available at https://www.regulations.gov by searching for Docket ID NRC-2025-1303. You may submit comments on the draft regulatory guidance using the methods provided in the ADDRESSES section of this document.

Draft Regulatory Guides DG-5087, “Standard Format and Content of Safeguards Contingency Plans for Nuclear Power Plants” (proposed Revision 2 to RG 5.54), and DG-5094, “Physical Protection Programs at Nuclear Power Reactors” (proposed Revision 2 to RG 5.76), contain SGI and are therefore withheld from public disclosure. In accordance with NRC policy, these DGs will be made available only to affected licensees and cleared stakeholders who have an established “need-to-know” and meet the access requirements of § 73.22(b). Because the majority of the changes to these DGs are limited to conforming changes needed to align with this proposed rulemaking, and considering the level of information provided in this notice, the NRC has determined that access to these DGs is not necessary for the general public to offer informed comment on the proposed rule. The publicly available draft guidance documents supporting this rulemaking are:

- DG-5069, “Fitness-For-Duty Programs at New Reactor Construction Sites,” proposed Revision 1 to RG 5.84;
- DG-5085, “Cybersecurity Programs for Nuclear Power Reactors,” proposed Revision 2 to RG 5.71;
- DG-5088, “Physical Protection of Special Nuclear Material of Moderate or Low Strategic Significance,” proposed Revision 2 to RG 5.59;
- DG-5089, “Security Event Notifications, Reports, and Records,” proposed Revision 4 to RG 5.62;
- DG-5090, “Access Authorization Program for Nuclear Power Plants,” proposed Revision 3 to RG 5.66;
- DG-5093, “Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities,” proposed Revision 2 to RG 5.75;
- DG-5095, “Insider Mitigation Program,” proposed Revision 2 to RG 5.77;

- DG-5097, “Preemption Authority, Enhanced Weapons Authority, and Firearms Background Checks,” proposed Revision 2 to RG 5.86;
- DG-5098, “Suspicious Activity Reports Under 10 CFR Part 73,” proposed Revision 2 to RG 5.87;
- DG-5099, “Fatigue Management for Nuclear Power Plant Personnel,” proposed Revision 1 to RG 5.73;
- DG-5102, “Protection of Safeguards Information,” proposed Revision 1 to RG 5.79;
- DG-5103, “Establishing Risk-Informed and Technology-Inclusive Cybersecurity Programs for Commercial Nuclear Plants,” proposed Revision 1 to RG 5.96; and
- DG-5104, “Access Authorization Program for Commercial Nuclear Plants,” proposed Revision 1 to RG 5.95.

The NRC is proposing to withdraw RG 5.83, “Cybersecurity Event Notifications.” As discussed in Section IV.C.(x), “Cybersecurity,” of this document, the NRC is proposing to eliminate specific cyber event notification requirements under § 73.77 and instead redirect licensees to established notification processes under parts 50, 53, and 73. RG 5.62 would be updated to include cybersecurity event notifications.

The NRC is proposing to withdraw NUREG-1304, “Reporting of Safeguards Events.” NUREG-1304, Revision 0, was temporarily withdrawn following publication of the NRC’s final rule on “Enhanced Weapons, Firearms Background Checks, and Security Event Notifications” (88 FR 15864; March 14, 2023). At that time, the NRC indicated its intent to conduct a public workshop after implementation of the new regulations in §§ 73.1200, 73.1205, and 73.1210, and to issue the workshop results as NUREG-1304, Revision 1. In light of the proposed regulatory changes in this rulemaking and the accompanying proposed updates to the associated guidance, the NRC has determined that NUREG-1304 is no longer necessary and proposes to withdraw the NUREG.

XVI. Availability of Documents

The documents identified in the following table are available to interested persons through one or more of the following methods, as indicated.

DOCUMENT	ADAMS Accession No. / Web link / *Federal Register* Citation
Proposed Rule Documents	
Regulatory Analysis for the Proposed Rule—Modernizing Security Requirements, June 2026	ML26113A051.
Draft Environmental Assessment for the Proposed Rule—Modernizing Security Requirements, June 2026	ML26113A050.
Backfitting and Issue Finality Assessment for the Proposed Rule—Modernizing Security Requirements, June 2026	ML26113A052.
Combined OMB Supporting Statement for Information Collections Contained in Modernizing Security Requirements Proposed Rule, June 2026	ML25309A008.
OMB Clearance Burden Tables for Modernizing Security Requirements Proposed Rule	ML26113A021.
Unofficial Redline Rule Language for the Proposed Rule—Modernizing Security Requirements, June 2026	ML25267A040.
Draft Regulatory Guidance Documents	
DG-5069, “Fitness-For-Duty Programs at New Reactor Construction Sites,” Revision 1 to RG 5.84, June 2026	ML21159A141.
DG-5085, “Cybersecurity Programs for Nuclear Power Reactors,” Revision 2 to RG 5.71, June 2026	ML24051A205.
DG-5088, “Physical Protection of Special Nuclear Material of Moderate or Low Strategic Significance,” Revision 2 to RG 5.59, June 2026	ML25233A199.
DG-5089, “Security Event Notifications, Reports, and Records,” Revision 4 to RG 5.62, June 2026	ML25233A197.
DG-5090, “Access Authorization Program for Nuclear Power Plants,” Revision 3 to RG 5.66, June 2026	ML21145A433.
DG-5093, “Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities,” Revision 2 to RG 5.75, June 2026	ML25233A188.

DG-5095, “Insider Mitigation Program,” Revision 2 to RG 5.77, June 2026	ML25233A187.
DG-5097, “Preemption Authority, Enhanced Weapons Authority, and Firearms Background Checks,” Revision 2 to RG 5.86, June 2026	ML25234A200.
DG-5098, “Suspicious Activity Reports Under 10 CFR Part 73,” Revision 2 to RG 5.87, June 2026	ML25233A184.
DG-5099, “Fatigue Management for Nuclear Power Plant Personnel,” Revision 1 to RG 5.73, June 2026	ML25233A183.
DG-5102, “Protection of Safeguards Information,” Revision 1 to RG 5.79, June 2026	ML25234A198.
DG-5103, “Establishing Risk-Informed and Technology-Inclusive Cybersecurity Programs for Commercial Nuclear Plants,” Revision 1 to RG 5.96, June 2026	ML25307A090.
DG-5104, “Access Authorization Program for Commercial Nuclear Plants,” Revision 1 to RG 5.95, June 2026	ML25318A144.
Other References	
Executive Order 12866, “Regulatory Planning and Review,” October 4, 1993	58 FR 51735.
Executive Order 14154, “Unleashing American Energy,” January 29, 2025	90 FR 8353.
Executive Order 14156, “Declaring a National Energy Emergency,” January 29, 2025	90 FR 8433.
Executive Order 14192, “Unleashing Prosperity Through Deregulation,” February 6, 2025	90 FR 9065.
Executive Order 14215, “Ensuring Accountability for All Agencies,” February 24, 2025	90 FR 10447.
Executive Order 14267, “Reducing Anti-Competitive Regulatory Barriers,” April 15, 2025	90 FR 15629.
Executive Order 14270, “Zero-Based Regulatory Budgeting to Unleash American Energy,” April 15, 2025	90 FR 15643.
Executive Order 14300, “Ordering the Reform of the Nuclear Regulatory Commission,” May 29, 2025	90 FR 22587.
Federal Register Notice—Final Rule, “Risk-Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors,” March 30, 2026	91 FR 15696.

Federal Register Notice—Direct Final Rule, "The Sunset Rule," December 3, 2025	90 FR 55621.
Federal Register Notice—"Mandatory Guidelines for Federal Workplace Drug Testing Programs," October 12, 2023	88 FR 70768.
Federal Register Notice—"Mandatory Guidelines for Federal Workplace Drug Testing Programs," October 12, 2023	88 FR 70814.
Federal Register Notice—Final Rule, "Procedures for Transportation Workplace Drug and Alcohol Testing Programs: Addition of Oral Fluid Specimen Testing for Drugs," May 2, 2023	88 FR 27596.
Federal Register Notice—Final Rule, "Enhanced Weapons, Firearms Background Checks, and Security Event Notifications," March 14, 2023	88 FR 15864.
Federal Register Notice—Final Rule, "Fitness for Duty Drug Testing Requirements," November 22, 2022	87 FR 71422.
Federal Register Notice—Proposed Rule, "Regulatory Improvements for Production and Utilization Facilities Transitioning to Decommissioning," March 3, 2022	87 FR 12254.
Federal Register Notice—Exemption, "Southern Nuclear Operating Company Inc; Vogtle Electric Generating Plant Units 3 and 4," December 28, 2021	86 FR 73809.
Federal Register Notice—Exemption, "Southern Nuclear Operating Company Inc; Vogtle Electric Generating Plant Units 3 and 4," November 29, 2021	86 FR 67734.
Federal Register Notice—Exemption, "Southern Nuclear Operating Company Inc; Vogtle Electric Generating Plant Units 3 and 4," June 12, 2019	84 FR 27364.
Federal Register Notice—Final Rule, "Procedures for Transportation Workplace Drug and Alcohol Testing Programs: Addition of Certain Schedule II Drugs to the Department of Transportation's Drug-Testing Panel and Certain Minor Amendments," November 13, 2017	82 FR 52229.
Federal Register Notice—Final Rule, "Fitness for Duty Programs," March 31, 2008	73 FR 16966.

Medical Review Officer Guidance Manual for Federal Workplace Drug Testing Programs (Effective February 1, 2024)	https://www.samhsa.gov/sites/default/files/mro-guidance-manual-2024.pdf.
NEI 08-09, Revision 7, “Cyber Security Plan for Nuclear Power Reactors,” April 2025	ML25107A191.
NRC Form 366 (Draft), “Licensee Event Report (LER)”	ML26020A117.
NRC Form 890, “Single Positive Test Form”	ML25044A086.
NRC Form 891, “Annual Reporting Form for Drug and Alcohol Tests”	ML26016A656.
NRC Form 891 (Draft), “Annual Reporting Form for Drug and Alcohol Tests”	ML26020A116.
NRC Letter, “Quad Cities Nuclear Power Station, Units 1 and 2 – Exemption from Select Requirements of 10 CFR Part 26 (EPID L-2020-LLE-0018 [COVID-19]),” April 8, 2020	ML20099A499.
NRC Memorandum, “Summary of July 31, 2025, Meeting with External Stakeholders Discussing Perspectives on Recent Security Event Notifications,” December 18, 2025	ML25351A137.
NUREG-2203, “Glossary of Security Terms for Nuclear Power Reactors,” February 2017	ML17047A669.
Petition for Rulemaking PRM 26-4 submitted by California Association of Marriage and Family Therapists, March 24, 2010, as supplemented by letters dated July 12, 2010, and July 26, 2010	ML102030370, ML102000432, and ML102250058.
Petition for Rulemaking PRM 26-7 submitted by Cheri Swensson on behalf of The American Academy of Health Care Providers in the Addictive Disorders, regarding Section 26.187(b)5 - Certification of Substance Abuse Expert, May 5, 2011	ML11256A020.
Petition for Rulemaking PRM 26-8 submitted by Thomas L. King regarding the Fitness for Duty Program, September 20, 2012	ML12332A137.
RG 5.62, Revision 3, “Physical Security Event Notifications, Reports, and Records,” September 2024	ML23299A176.
RG 5.86, Revision 1, “Preemption Authority, Enhanced Weapons	ML23299A173.

Authority, and Firearms Background Checks," April 2024	
RG 5.87, Revision 1, "Suspicious Activity Reports Under 10 CFR Part 73," May 2024	ML23299A172.
SECY-24-0011, "Final Rule: Regulatory Improvements for Production and Utilization Facilities Transitioning to Decommissioning (3150-AJ59; NRC-2015-0070)," January 31, 2024	ML23258A200.
SRM-SECY-16-0073, "Staff Requirements—SECY-16-0073—Options and Recommendations for the Force-on-Force Inspection Program in Response to SRM-SECY-14-0088," October 5, 2016	ML16279A345.
SRM-SECY-22-0052, "Staff Requirements—SECY-22-0052—Proposed Rule: Alignment of Licensing Processes and Lessons Learned from New Reactor Licensing (RIN 3150-AI66)," November 20, 2024	ML24326A003.

The NRC may post materials related to this document, including public comments, on the Federal rulemaking website at https://www.regulations.gov under Docket ID NRC-2025-1303. In addition, the Federal rulemaking website allows members of the public to receive alerts when changes or additions occur in a docket folder. To subscribe: 1) navigate to the docket folder (NRC-2025-1303); 2) click the "Subscribe" button; and 3) enter an email address and click on the "Subscribe" button.

List of Subjects

10 CFR Part 26

Administrative practice and procedure, Alcohol abuse, Alcohol testing, Appeals, Drug abuse, Drug testing, Employee assistance programs, Fitness for duty, Management actions, Nuclear power plants and reactors, Privacy, Protection of information, Radiation protection, Reporting and recordkeeping requirements.

10 CFR Part 50

Administrative practice and procedure, Antitrust, Backfitting, Classified information, Criminal penalties, Education, Emergency planning, Fire prevention, Fire protection, Intergovernmental relations, Nuclear power plants and reactors, Penalties, Radiation protection, Reactor siting criteria, Reporting and recordkeeping requirements, Whistleblowing.

10 CFR Part 52

Administrative practice and procedure, Antitrust, Combined license, Early site permit, Emergency planning, Fees, Inspection, Issue finality, Limited work authorization, Manufacturing license, Nuclear power plants and reactors, Probabilistic risk assessment, Prototype, Reactor siting criteria, Redress of site, Penalties, Reporting and recordkeeping requirements, Standard design, Standard design certification.

10 CFR Part 72

Administrative practice and procedure, Hazardous waste, Indians, Intergovernmental relations, Nuclear energy, Penalties, Radiation protection, Reporting and recordkeeping requirements, Security measures, Spent fuel, Whistleblowing.

10 CFR Part 73

Criminal penalties, Exports, Hazardous materials transportation, Imports, Incorporation by reference, Nuclear energy, Nuclear materials, Nuclear power plants and reactors, Penalties, Reporting and recordkeeping requirements, Security measures.

10 CFR Part 95

Classified information, Criminal penalties, Penalties, Reporting and recordkeeping requirements, Security measures.

For the reasons set out in the preamble and under the authority of the Atomic Energy Act of 1954, as amended; the Energy Reorganization Act of 1974, as amended; and 5 U.S.C. 552 and 553, the NRC is proposing to amend 10 CFR parts 26, 50, 52, 72, 73, and 95 as follows:

PART 26—FITNESS FOR DUTY PROGRAMS

1. The authority citation for part 26 continues to read as follows:

Authority: Atomic Energy Act of 1954, secs. 53, 103, 104, 107, 161, 223, 234, 1701 (42 U.S.C. 2073, 2133, 2134, 2137, 2201, 2273, 2282, 2297f); Energy Reorganization Act of 1974, secs. 201, 202 (42 U.S.C. 5841, 5842); 44 U.S.C. 3504 note.

2. In § 26.3, revise paragraphs (a) through (b) and the introductory text to (c) to read as follows:

§ 26.3 Scope.

(a) Licensees who are authorized to operate a nuclear power reactor under 10 CFR 50.57, and holders of a combined license under 10 CFR part 52 after the Commission has made the finding under 10 CFR 52.103(g) shall comply with the requirements of this part, except for subparts K and M of this part, and implement the FFD program before the initial fuel load into the reactor.

(b) Licensees who are authorized to possess, use, or transport formula quantities of strategic special nuclear material (SSNM) under part 70 of this chapter, and any corporation, firm, partnership, limited liability company, association, or other organization who obtains a certificate of compliance or an approved compliance plan under part 76 of this chapter, only if the entity elects to engage in activities involving formula quantities of SSNM, shall comply with the requirements of this part, except for subparts I, K, and M of this part.

(c) Before the initial fuel load into the reactor, the following licensees and other entities shall comply with the requirements of this part, except for subparts I and M of this part; and, no later than initial fuel load into the reactor, the following licensees and

other entities shall comply with the requirements of this part, except subpart M of this part:

* * * * *

3. In § 26.4:

a. Revise paragraphs (e)(1), (5), and (6)(iv) and (vii);

b. Add paragraph (e)(7);

c. Revise paragraph (f);

The revisions and addition read as follows:

§ 26.4 FFD program applicability to categories of individuals.

* * * * *

(e) * * *

(1) Serves as security personnel required by the NRC before the initial fuel load into the reactor, at which time individuals who serve as security personnel required by the NRC must meet the requirements applicable to security personnel in paragraph (a)(5) of this section;

* * * * *

(5) Supervises or manages the construction of safety- or security-related SSCs;

(6) * * *

(iv) Conducting background investigations or psychological assessments used by the licensee or other entity to make access authorization determinations, except that he or she shall be subject to behavioral observation only when he or she is present at the location where the nuclear power plant will be constructed and operated, and licensees and other entities may rely on a local hospital or other organization that meets the requirements of 49 CFR part 40 to collect his or her specimens for drug and alcohol testing;

* * * * *

(vii) Performing any of the activities or having any of the duties listed in paragraph (e)(6) of this section for any C/V upon whom the licensee's or other entity's access authorization program will rely; or

(7) Escorts an individual or small group of individuals, as determined by the licensee or other entity.

(f) Any individual who is constructing or directing the construction of safety- or security-related SSCs shall be subject to an FFD program that meets the requirements of subpart K, or, if applicable, subpart M of this part, unless the licensee or other entity subjects the individuals to an FFD program that meets all of the requirements of this part, except for subparts I, K, and M of this part, or if the individual is escorted.

* * * * *

4. In § 26.5:

a. Revise the definitions of "*Analytical run*", "*Cancelled test*", "*Cutoff level*", and "*Directing*";

b. Add the definition for "*Escort*";

c. Remove the definition of "*Licensee testing facility*";

d. Remove the definition of "*Questionable validity*";

e. Revise the definitions of "*Positive result*", and "*Rejected for testing*";

f. Add the definition for "*Sequestration event*"; and

g. Remove the definitions of "*Validity screening test*", and "*Validity screening test lot*".

The revisions and additions read as follows:

§ 26.5 Definitions.

* * * * *

Analytical run means the process of testing a group of urine specimens for validity or for the presence of drugs and/or drug metabolites. For the purposes of defining the periods within which performance testing must be conducted by any HHS-

certified laboratory that continuously processes specimens, an analytical run is defined as no more than an 8-hour period. For a facility that analyzes specimens in batches, an analytical run is defined as a group of specimens that are handled and tested together.

* * * * *

Cancelled test means the test result reported by the MRO to the licensee or other entity when a specimen has been reported to the MRO by the HHS-certified laboratory as an invalid result (for which the donor has no legitimate explanation), a specimen has been rejected for testing by the HHS-certified laboratory, or the retesting of a single specimen or the testing of Bottle B of a split specimen fails to reconfirm the original test result. For alcohol testing only, *cancelled test* means a test result that was not acceptable because testing did not meet the quality assurance and quality control requirements in § 26.91.

* * * * *

Cutoff level means the concentration or decision criteria established for designating and reporting a test result as positive, adulterated, substituted, dilute, or invalid (referring to initial or confirmatory test results from an HHS-certified laboratory).

* * * * *

Directing means the exercise of control over a work activity by an individual who is directly involved in the execution of the work activity, and either makes technical decisions for that activity without subsequent technical review or is ultimately responsible for the correct performance of that work activity.

* * * * *

Escort means a person who is designated by the licensee or other entity to be responsible for directly observing an individual who has been assigned to perform duties and responsibilities or maintain the type of access described in § 26.4(f) but is not subject to the requirements in this part.

* * * * *

Positive result means, for drug testing, the result reported by an HHS-certified laboratory when a specimen contains a drug or drug metabolite equal to or greater than the cutoff concentration. A result reported by an HHS-certified laboratory that a specimen contains a drug or drug metabolite below the cutoff concentration is also a positive result when the laboratory has conducted the special analysis permitted in § 26.163(a)(2). For alcohol testing, a positive result means the result reported by a collection site when the BAC indicated by testing a specimen is equal to or greater than the cutoff concentrations established in this part.

* * * * *

Rejected for testing means the result reported to the MRO by an HHS-certified laboratory when no tests can be performed on a specimen.

* * * * *

Sequestration event means a situation in which personnel remain on-site at a nuclear power reactor due to unavoidable external conditions that pose a risk to the safe, secure, and continuous operation of the facility.

* * * * *

§ 26.8 [Amended]

5. In § 26.8(b), remove the references “26.125, 26.127, 26.129, 26.135, 26.137, 26.139,”.

6. In § 26.27, revise paragraph (c)(4), and add new paragraph (c)(5) to read as follows:

§ 26.27 Written policy and procedures

* * * * *

(c) * * *

(4) Describe the process to be followed if an individual’s behavior raises a concern regarding the possible use, sale, or possession of illegal drugs on or off site; the

possible possession or consumption of alcohol on site; or impairment from any cause which in any way could adversely affect the individual's ability to safely and competently perform his or her duties. The procedure must require that individuals who have an FFD concern about another individual's behavior shall contact the personnel designated in the procedures to report the concern; and

(5) For licensees and other entities that allow escorting of individuals performing activities described in 10 CFR 26.4(f), but do not implement an FFD program under subpart K or subpart M during construction, describe the process that the licensee or other entity will use for the processing, escorting, and control of individuals under escort and the duties and responsibilities of escorts.

7. In § 26.29, revise the first sentence of paragraph (c)(2) to read as follows:

§ 26.29 Training.

* * * * *

(c) * * *

(2) Individuals shall complete refresher training on a nominal 24-month frequency, or more frequently where the need is indicated. Indications of the need for more frequent training include, but are not limited to, an individual's failure to properly implement FFD program procedures and the frequency, nature, or severity of problems discovered through audits or the administration of the program. * * *

* * * * *

8. In § 26.31, revise paragraphs (b)(1)(v) and (d)(2)(vii), the introductory text to paragraph (d)(2)(i), and (d)(3)(i); remove paragraph (d)(3)(ii); revise and redesignate paragraph (d)(3)(iii) as paragraph (d)(3)(ii) to read as follows:

§ 26.31 Drug and alcohol testing.

* * * * *

(b) * * *

(1) * * *

(v) FFD program personnel shall be subject to a behavioral observations program designed to assure that they continue to meet the highest standards of honesty and integrity. The MRO, MRO staff, and SAE shall be subject to behavioral observation when on site at a licensee's or other entity's facility.

* * * * *

(d) * * *

(2) * * *

(i) Be administered in a manner that provides reasonable assurance that individuals are unable to predict the time periods during which specimens will be collected. At a minimum, the FFD program must—

* * * * *

(vii) Ensure that the number of random tests performed annually meets the sampling requirements described in § 26.31(d)(2)(vii)(A) and (B), or in § 26.31(d)(2)(vii)(C) when applicable.

(A) Random tests must be performed annually for at least 50 percent of the population of individuals subject to the FFD program that is comprised of all contractors/vendors and the following licensee employees: those who are licensed under 10 CFR part 55 to operate a power reactor, security personnel under § 26.4(a)(5), FFD program personnel under § 26.4(g), and supervisory personnel directing the operation or maintenance of safety- or security-related SSCs or directing the performance of security duties under § 26.4(a)(5).

(B) Random tests must be performed annually for at least 25 percent of the licensee employee population subject to the FFD program that is not covered by random testing performed under § 26.31(d)(2)(vii)(A).

(C) If the number of individuals subject to random testing is such that § 26.31(d)(2)(vii)(A) and (B) cannot be implemented without predictable outcomes, then

the licensee or other entity must use a C/TPA to manage the random testing pool and make selections for testing throughout the year. In such instances, the C/TPA must ensure that testing rates for the random testing pool from which they sample meet the requirements described in § 26.31(d)(2)(vii)(A) and (B).

(3) * * *

(i) Testing of specimens collected under § 26.83(b) must be performed in a laboratory that is certified by HHS for that purpose, consistent with its standards and procedures for certification. Urine specimens sent to HHS-certified laboratories must be subject to initial validity and initial drug testing by the laboratory. Oral fluid specimens sent to HHS-certified laboratories must be subject to initial drug testing by the laboratory. Specimens for initial validity or initial drug testing that yield positive, positive and dilute, adulterated, substituted, or invalid test results must be subject to confirmatory testing by the laboratory, except for invalid specimens that cannot be tested. Licensees and other entities shall ensure that laboratories report results for all specimens sent for testing, including blind performance test samples.

(ii) At a minimum, licensees and other entities shall apply the cutoff levels specified in § 26.163(a)(1) for initial drug testing and in § 26.163(b)(1) for confirmatory drug testing at the HHS-certified laboratory. At their discretion, licensees and other entities may implement programs with lower cutoff levels in testing for drugs and drug metabolites.

* * * * *

9. Revise § 26.33 to read as follows:

§ 26.33 Behavioral observation.

(a) Licensees and other entities shall ensure that the individuals who are subject to this subpart are subject to behavioral observation.

(b) Behavioral observation must be performed by individuals who are trained under § 26.29 to detect behaviors that may indicate possible use, sale, or possession of

illegal drugs; use or possession of alcohol on site or while on duty; or impairment from fatigue or any cause that, if left unattended, may constitute a risk to public health and safety or the common defense and security.

(c) Individuals who are subject to this subpart shall report any FFD concerns about other individuals to the personnel designated in the FFD policy.

§ 26.37 [Amended]

10. In § 26.37(e), remove the phrase “C/Vs providing specimen collection services, and licensee testing facility procedures, must” and add in its place the phrase “C/Vs providing specimen collection services must”.

11. In § 26.41, revise and republish paragraphs (a), (c), and (g) to read as follows:

§ 26.41 Audits and corrective action.

(a) *General.* Each licensee and other entity who is subject to this subpart is responsible for the continuing effectiveness of the FFD program, including FFD program elements that are provided by C/Vs, the FFD programs of any C/Vs that are accepted by the licensee or other entity, and any FFD program services that are provided to the C/V by a subcontractor. Each licensee and other entity shall ensure that these programs are audited and that corrective actions are taken to resolve any problems identified.

* * * * *

(c) C/Vs.

(1) FFD services that are provided to a licensee or other entity by C/V personnel who are off site or are not under the direct daily supervision or observation of the licensee’s or other entity’s personnel must be audited on a nominal 12-month frequency.

(2) Licensees and other entities need not audit organizations and professionals who may provide an FFD program service to the licensee or other entity, but who are not

routinely involved in providing services to a licensee's or other entity's FFD program, as specified in § 26.4(i)(1).

* * * * *

(g) *Sharing of audits.* Licensees and other entities may jointly conduct audits, or may accept audits of C/Vs that were conducted by other licensees and entities who are subject to this subpart, if the audit addresses the services obtained from the C/V by each of the sharing licensees and other entities.

(1) Licensees and other entities shall review audit records and reports to identify any areas that were not covered by the shared or accepted audit.

(2) Licensees and other entities shall ensure that FFD program elements and services on which the licensee or entity relies are audited, if the program elements and services were not addressed in the shared audit.

(3) Sharing licensees and other entities need not re-audit the same C/V for the same period of time.

(4) Each sharing licensee and other entity shall maintain a copy of the shared audit, including findings, recommendations, and corrective actions.

12. In § 26.75, revise paragraph (h) and remove and reserve paragraph (i) to read as follows:

§ 26.75 Sanctions.

* * * * *

(h) A licensee or other entity may not terminate an individual's authorization and may not subject the individual to other administrative action based solely on a positive drug test result that has not been reviewed by the MRO under § 26.185, unless other evidence, including information obtained under the process set forth in § 26.189, indicates that the individual is impaired or might otherwise pose a safety hazard.

(i) [Reserved]

13. In § 26.83, revise paragraph (b) to read as follows:

§ 26.83 Specimens to be collected.

* * * * *

(b) Collect only urine or oral fluid specimens for both initial and confirmatory tests for drugs.

(1) For each condition for testing under § 26.31(c), the licensee or other entity shall establish through its policy and procedures when a urine or oral fluid specimen is to be collected.

(2) For each observed collection condition under § 26.115(a), the licensee or other entity shall always collect and test the same specimen type.

14. In § 26.109, revise paragraph (a) to read as follows:

§ 26.109 Urine specimen quantity.

* * * * *

(a) Licensees and other entities who are subject to this subpart shall establish a predetermined quantity of urine that donors are requested to provide when submitting a specimen. At a minimum, the predetermined quantity must include 30 milliliters (mL) to ensure that a sufficient quantity of urine is available for initial and confirmatory validity and drug tests at an HHS-certified laboratory, and for retesting of an aliquot of the specimen if requested by the donor under § 26.165(b). The licensee’s or other entity’s predetermined quantity may include more than 30 mL, if the testing program follows split specimen procedures or tests for additional drugs. Where collected specimens are to be split under the provisions of this subpart, the predetermined quantity must include an additional 15 mL.

* * * * *

15. In § 26.111, revise paragraph (d) to read as follows:

§ 26.111 Checking the acceptability of the urine specimen.

* * * * *

(d) Any specimen of 15 mL or more that the collector suspects has been diluted, substituted, or adulterated, and any specimen of 15 mL or more that has been collected under direct observation under paragraph (c) of this section, must be sent to the HHS-certified laboratory for testing.

* * * * *

16. In § 26.113, revise paragraph (c) to read as follows:

§ 26.113 Splitting the urine specimen.

* * * * *

(c) Licensees and other entities may use aliquots of the specimen collected for initial validity and drug testing, as permitted under § 26.31(d)(3)(ii), or to test for additional drugs, as permitted under § 26.31(d)(1)(i)(A), but only if sufficient urine is available for this testing after the specimen has been split into Bottle A and Bottle B.

17. In § 26.117, revise paragraphs (f), (g), (h), (i) and (j) to read as follows:

§ 26.117 Preparing drug testing specimens for storage and shipping.

* * * * *

(f) The specimens and Federal CCFs must be packaged for transfer to the HHS-certified laboratory. If the specimens are not immediately prepared for transfer, they must be appropriately safeguarded during temporary storage.

(g) While any part of the chain of custody procedures is being performed, the specimens and custody documents must be under the control of the involved collector, except as provided in § 26.109(b)(1)(ii) for the Federal CCF. The collector may not leave the collection site during the interval between presentation of the specimen by the donor and securing of the specimens with identifying labels bearing the donor’s specimen identification numbers and seals initialed by the donor. If the involved collector momentarily leaves his or her workstation, the sealed specimens and Federal CCFs

must be secured or taken with him or her. If the collector is leaving for an extended period of time, the specimens must be packaged for transfer to the HHS-certified laboratory and secured before the collector leaves the collection site.

(h) The specimen(s) sealed in a shipping container must be immediately transferred, appropriately safeguarded during temporary storage, or kept under the personal control of an authorized individual until transferred. These minimum procedures apply to the shipping of specimens to HHS-certified laboratories. As an option, licensees and other entities may ship several specimens by courier in a locked or sealed shipping container.

(i) Collection site personnel shall ensure that a Federal CCF is packaged with its associated specimen bottle. The sealed and labeled specimen bottles, with their associated Federal CCFs that are being transferred from the collection site to the HHS-certified laboratory, must be placed in a second, tamper-evident shipping container. The second container must be designed to minimize the possibility of damage to the specimen during shipment (e.g., specimen boxes, shipping bags, padded mailers, or bulk insulated shipping containers with that capability), so that the contents of the shipping containers are no longer accessible without breaking a tamper-evident seal.

(j) Collection site personnel shall arrange to transfer the collected specimens to the HHS-certified laboratory. Licensees and other entities shall take appropriate and prudent actions to minimize false negative results from specimen degradation. Urine specimens that have not shipped to the HHS-certified laboratory within 24 hours of collection and any urine specimen that is suspected of having been substituted, adulterated, or tampered with in any way must be maintained cooled to not more than 6 °C (42.8 °F) until they are shipped to the HHS-certified laboratory. Oral fluid specimens shall be stored under the conditions specified by the oral fluid specimen collection device manufacturer. Specimens must be shipped from the collection site to the HHS-certified laboratory as soon as reasonably practical but, except under unusual circumstances, the

time between specimen shipment and receipt of the specimen at the HHS-certified laboratory should not exceed 2 business days.

* * * * *

§ 26.119 [Amended]

18. In § 26.119(a), remove the phrase “within 5 business days” and add in its place the phrase “within 5 business days (can be extended to 10 business days if a justification acceptable to the MRO is provided by the donor and documented by the MRO)”.

Subpart F [Reserved]

19. Remove and reserve subpart F.

20. In § 26.153, revise paragraph (f)(2) to read as follows:

§ 26.153 Using certified laboratories for testing specimens.

* * * * *

(f) * * *

(2) The laboratory shall make available qualified personnel to testify in an administrative or disciplinary proceeding against an individual when that proceeding is based on test results reported by the HHS-certified laboratory;

* * * * *

§ 26.159 [Amended]

21. In § 26.159(b)(1)(ii), remove the last sentence.

22. In § 26.165, revise paragraphs (a), (b)(5), and (f)(2) to read as follows:

§ 26.165 Testing split specimens and retesting single specimens.

(a) Testing split specimens.

(1) If a specimen has been split into Bottle A and Bottle B at the collection site, the HHS-certified laboratory shall perform initial and confirmatory validity and drug testing, if required, on the specimen in Bottle A.

(2) If the specimen in Bottle A is free of any evidence of drugs or drug metabolites, and is a valid specimen, then the HHS-certified laboratory may discard the specimens in Bottles A and B.

(b) * * *

(5) As soon as reasonably practical and not more than 1 business day following the day of the donor's request, as permitted in paragraph (b)(3) or (b)(4) of this section, the MRO shall ensure that the HHS-certified laboratory forwards an aliquot of a single specimen or Bottle B of a split specimen (as appropriate), to a second HHS-certified laboratory that did not test the specimen in Bottle A.

* * * * *

(f) * * *

(2) If a donor requests that Bottle B be tested or that an aliquot of the single specimen be retested, and either Bottle B or the single specimen are not available due to circumstances outside of the donor's control (including, but not limited to, circumstances in which there is an insufficient quantity of the single specimen or the specimen in Bottle B to permit retesting, either Bottle B or the original single specimen is lost in transit to the second HHS-certified laboratory, or Bottle B has been lost at the HHS-certified laboratory), the MRO shall cancel the test, report a cancelled test result to the licensee or other entity for the donor's specimen, and inform the licensee or other entity that another collection is required under direct observation as soon as reasonably practical. The donor shall receive no notice of the collection requirement before he or she is instructed to proceed to the collection site. The licensee or other entity shall continue to administratively withdraw the individual's authorization, as required by § 26.165(f)(1) until the results of the second specimen collection have been received by the MRO. The licensee or other entity shall eliminate from the donor's personnel and

other records any matter that could link the donor to the original positive, adulterated, or substituted test result(s) and any temporary administrative action, and may not impose any sanctions on the donor for a cancelled test. If test results from the second specimen collected are positive, adulterated, or substituted and the MRO determines that the donor has violated the FFD policy, the licensee or other entity shall impose the appropriate sanctions specified in subpart D of this part, but may not consider the original confirmed positive, adulterated, or substituted test result that was reported as a cancelled test by the MRO under § 26.159(b)(2) in determining the appropriate sanctions.

23. In § 26.167, revise paragraph (d)(1) to read as follows:

§ 26.167 Quality assurance and quality control.

* * * * *

(d) * * *

(1) Any initial drug test performed by an HHS-certified laboratory must use an immunoassay or an alternate technology that is permitted for use in Federal workplace drug testing programs for this purpose.

* * * * *

24. In § 26.168, revise paragraphs (a) through (d), (f), and (i)(1) through (3) to read as follows:

§ 26.168 Blind performance testing.

(a) Each licensee and other entity shall submit blind performance test samples to each HHS-certified laboratory under contract to perform specimen testing.

(1) A licensee or other entity may submit blind performance test samples for each site (e.g., a location with one or more nuclear power reactors) or for its entire fleet (e.g., nuclear power reactors at multiple sites), as applicable.

(2) In each calendar quarter, the number of blind performance test samples submitted must be a minimum of one percent of all specimens (up to a maximum of 100) or ten blind performance test samples, whichever is greater.

(3) In each calendar quarter, licensees and other entities should attempt to submit blind performance test samples at a frequency that corresponds to the submission frequency for other specimens.

(b) Approximately 60 percent of the blind performance test samples submitted to the HHS-certified laboratory must be positive for one or more drugs or drug metabolites per sample and submitted so that all of the drugs for which the FFD program is testing are included at least once each calendar quarter.

(c) The positive blind performance test samples must be positive for only those drugs for which the FFD program is testing and formulated at concentrations established in paragraph (g)(2) of this section.

(d) To challenge the HHS-certified laboratory's ability to limit false negatives, approximately 10 percent of the blind performance test samples submitted to the laboratory each quarter or at least one sample per quarter, whichever is greater, must be formulated at the concentrations established in paragraph (g)(3) of this section.

* * * * *

(f) Approximately 10 percent of the blind performance test samples submitted to the HHS-certified laboratory each quarter or at least one sample per quarter, whichever is greater, must be negative, as specified in paragraph (g)(1) of this section.

* * * * *

(i) * * *

(1) The licensee or other entity shall submit blind performance test samples to the HHS-certified laboratory using the same channels (i.e., from the licensee's or other entity's collection site) through which donors' specimens are sent to the laboratory;

(2) The collector shall use a Federal CCF, place fictional initials on the specimen bottles' labels/seals, and indicate for the MRO on the MRO's copy that the specimen is a blind performance test sample; and

(3) The licensee or other entity shall ensure that all blind performance test samples include split samples, when the FFD program includes split specimen procedures.

25. In § 26.169, revise paragraphs (h)(4) through (7) to read as follows:

§ 26.169 Reporting Results.

* * * * *

(h) * * *

(4) Number of specimens reported as adulterated;

(5) Number of specimens reported as substituted;

(6) Number of specimens reported as positive and dilute;

(7) Number of specimens reported as invalid; and

* * * * *

26. In § 26.183, revise paragraph (a), revise the introductory text to paragraph (b), and revise paragraphs (c), (d)(2)(ii), (iii), and (iv) to read as follows:

§ 26.183 Medical review officer.

(a) *Qualifications.* The MRO shall be knowledgeable of this part and of the FFD policies of the licensees and other entities for whom the MRO provides services. The MRO shall be a physician holding either a Doctor of Medicine or Doctor of Osteopathy degree, or an equivalent foreign degree, and who is licensed to practice medicine by any State or Territory of the United States, the District of Columbia, or the Commonwealth of Puerto Rico. The MRO shall have passed an examination administered by a nationally-recognized MRO certification board or subspecialty board for medical practitioners in the field of medical review of Federally mandated drug tests.

(b) *Relationships.* The MRO may be an employee of the licensee or other entity or a contractor. However, the MRO may not be an employee or agent of, or have any financial interest in, an HHS-certified laboratory for whom the MRO reviews drug test results. Additionally, the MRO may not derive any financial benefit by having the licensee or other entity use a specific drug testing laboratory and may not have any agreement with such parties that may be construed as a potential conflict of interest. Examples of relationships between laboratories and MROs that create conflicts of interest, or the appearance of such conflicts, include, but are not limited to—

* * * * *

(c) *Responsibilities.* The primary role of the MRO is to review and interpret positive, positive and dilute, adulterated, substituted, and invalid results obtained through the licensee's or other entity's testing program and to identify any evidence of subversion of the testing process. The MRO is also responsible for identifying any issues associated with collecting and testing specimens, and for advising and assisting FFD program management in planning and overseeing the overall FFD program.

(1) In carrying out these responsibilities, the MRO shall examine alternate medical explanations for any positive, positive and dilute, adulterated, substituted, or invalid test result. This action may include, but is not limited to, conducting a medical interview with the donor, reviewing the donor's medical history, or reviewing any other relevant biomedical factors. The MRO shall review all medical records that the donor may make available when a positive, positive and dilute, adulterated, substituted, or invalid test result could have resulted from responsible use of legally prescribed medication, a documented condition or disease state, or the demonstrated physiology of the donor.

(2) The MRO may only consider the results of tests of specimens that are collected and processed under this part, including the results of testing split specimens, in making his or her determination, as long as those split specimens have been stored and tested under the procedures described in this part.

(d) * * *

(2) * * *

(ii) The staff reviews of positive, positive and dilute, adulterated, substituted, and invalid test results must be limited to reviewing the Federal CCF to determine whether it contains any errors that may require corrective action and to ensure that it is consistent with the information on the MRO's copy. The staff may resolve errors in Federal CCFs that require corrective action(s), but shall forward the Federal CCFs to the MRO for review and approval of the resolution.

(iii) The staff may not conduct interviews with donors to discuss positive, positive and dilute, adulterated, substituted, or invalid test results nor request medical information from a donor. Only the MRO may request and review medical information related to a positive, positive and dilute, adulterated, substituted, or invalid test result or other matter from a donor.

(iv) Staff may not report nor discuss with any individuals other than the MRO and other MRO staff any positive, positive and dilute, adulterated, substituted, or invalid test results received from the HHS-certified laboratory before those results have been reviewed and confirmed by the MRO. Any MRO staff discussions of confirmed positive, adulterated, substituted, invalid, or dilute test results must be limited to discussions only with the licensee's or other entity's FFD program personnel and may not reveal quantitative test results or any personal medical information about the donor that the MRO may have obtained in the course of reviewing confirmatory test results from the HHS-certified laboratory.

27. In § 26.185, revise paragraphs (b), (j)(3), and (m) to read as follows:

§ 26.185 Determining a fitness-for-duty policy violation.

* * * * *

(b) *Reporting of initial test results prohibited.* Neither the MRO nor MRO staff may report positive, positive and dilute, adulterated, substituted, or invalid initial test results that are received from the HHS-certified laboratory to the licensee or other entity.

* * * * *

(j) * * *

(3) If the MRO determines that the donor has used another individual's prescription medication, the MRO shall report to the licensee that the donor has violated the FFD policy.

* * * * *

(m) *Result scientifically insufficient.* Based on the review of inspection and audit reports, quality control data, multiple specimens, and other pertinent results, the MRO may determine that a positive, adulterated, substituted or invalid test result is scientifically insufficient for further action and may declare that a drug or validity test result is not an FFD policy violation, but that a negative test result was not obtained. In this situation, the MRO may request retesting of the original specimen before making this decision. The MRO is neither expected nor required to request such retesting, unless in the sole opinion of the MRO, such retesting is warranted. The MRO may request that the reanalysis be performed by the same laboratory, or that an aliquot of the original specimen be sent for reanalysis to another HHS-certified laboratory. The HHS-certified laboratory shall assist in this review process, as requested by the MRO, by making available the individual(s) responsible for day-to-day management of the HHS-certified laboratory, or other individuals who are forensic toxicologists or who have equivalent forensic experience in urine drug testing, to provide specific consultation as required by the MRO.

* * * * *

28. In § 26.187, revise paragraph (b)(4); redesignate paragraph (b)(5) as paragraph (b)(6) and add new paragraph (b)(5); and revise the introductory text to paragraph (g)(1) to read as follows:

§ 26.187 Substance abuse expert.

* * * * *

(b) * * *

(4) A licensed or certified employee assistance professional;

(5) A State-licensed or -certified marriage and family therapist; or

* * * * *

(g) * * *

(1) The SAE shall make determinations of fitness in at least the following three circumstances:

* * * * *

29. In § 26.189, revise the introductory text to paragraph (c) to read as follows:

§ 26.189 Determination of fitness.

* * * * *

(c) A determination of fitness that is conducted for cause (i.e., because of observed behavior or a physical condition) must be conducted through face-to-face interaction between the subject individual and the professional making the determination. An electronic means of communication (i.e., video teleconference technology) may be used as long at the communication method provides sufficient visual and aural clarity to complete the assessment. A determination of fitness that is performed by electronic means must be supported by someone who is present in-person with the individual being assessed only for for-cause drug and alcohol testing determinations under § 26.31(c)(2) and fatigue assessments performed for cause under § 26.211(a)(1). The supporting person must be trained in accordance with the requirements in § 26.29.

* * * * *

§ 26.202 [Reserved].

30. In § 26.202, remove and reserve paragraph (e).

31. In § 26.203, revise paragraphs (d)(4) and (5), add paragraph (d)(6), remove paragraph (e), and redesignate paragraph (f) as paragraph (e).

The revisions and additions read as follows:

§ 26.203 General provisions.

* * * * *

(d) * * *

(4) The documentation of work hour reviews that is required in § 26.205(e)(3) and (e)(4);

(5) The documentation of fatigue assessments that is required in § 26.211(g); and

(6) The documentation of utilization of the exception for sequestration events that is required in § 26.207(e)(3), including the bases for utilization of the exception.

* * * * *

32. In § 26.207, revise the last sentence in paragraph (a)(1)(ii), and add paragraph (e) to read as follows:

§ 26.207 Waivers and exceptions.

(a) * * *

(1) * * *

(ii) * * * For licensees and other entities in § 26.3(a), (c), (d), and (f), the assessment may be performed remotely using electronic communications. In such instances, the assessment must be supported by someone who is present in-person with the individual whose alertness may be impaired, and that supporting person must

be trained under the requirements of either §§ 26.29 and 26.203(c) or §§ 26.202(c) and 26.608.

* * * * *

(e) *Sequestration events*. During a sequestration event as defined in § 26.5, a licensee may follow the requirements in § 26.207(e)(1) through (4) as an alternative to the requirements of § 26.205(c) and (d). If a licensee chooses to utilize these alternative requirements during a sequestration event, then the licensee must follow the requirements in § 26.207(e)(1) through (4) until the conclusion of the sequestration event.

(1) During the sequestration event, the licensee shall implement alternative work hour controls and fatigue management measures that provide reasonable assurance that personnel sequestered on site will continue to meet the performance objectives of § 26.23(e) for the duration of the sequestration event.

(2) During the sequestration event, the licensee shall implement alternative work hour controls that, at a minimum, ensure:

(i) Individuals shall not work more than 16 hours in any 24-hour period and not more than 86 hours in any 7-day period, excluding shift turnover time;

(ii) A minimum 10-hour break is provided between successive work periods;

(iii) 12-hour shifts are limited to no more than 14 consecutive days;

(iv) A minimum of 6 days off is provided in any rolling 30-day period;

(3) Licensees shall document the bases for invoking a sequestration event exception.

(4) Licensees shall restore compliance with § 26.205(c) and (d) as soon as practicable following the conclusion of a sequestration event, but no more than 60 days following the start of the event.

33. In § 26.211, revise the last sentence in the introductory text to paragraph (b) to read as follows:

§ 26.211 Fatigue assessments.

* * * * *

(b) * * * For licensees and other entities in § 26.3(a), (c), (d), and (f), a fatigue assessment may be performed remotely using electronic communications. In such instances, the fatigue assessment must be supported by someone who is present in-person with the individual whose alertness may be impaired, and that supporting person must be trained in accordance with the requirements of either §§ 26.29 and 26.203(c) or §§ 26.202(c) and 26.608.

* * * * *

34. In § 26.401, revise paragraph (b) to read as follows:

§ 26.401 General.

* * * * *

(b) Licensees and other entities who intend to implement an FFD program under this subpart shall submit a description of the FFD program and its implementation as part of the license, permit, or limited work authorization application.

* * * * *

35. In § 26.403, revise paragraph (a) and add paragraph (b)(4) to read as follows:

§ 26.403 Written policy and procedures.

(a) Licensees and other entities who implement an FFD program under this subpart shall ensure that a clear, concise, written FFD policy statement is provided to individuals who are subject to the program or escorted. The policy statement must be written in sufficient detail to provide affected individuals with information on what is expected of them and what consequences may result from a lack of adherence to the policy.

(b) * * *

(4) The processing, escorting, and control of individuals under escort and the duties and responsibilities of escorts.

36. In § 26.405:

a. Revise the introductory text to paragraph (c)(3);

b. In paragraph (d), remove the phrase “urine are collected” and add in its place the phrase “those collected under § 26.83(b)”; and

d. Revise paragraphs (f) and (g).

The revisions and addition read as follows:

§ 26.405 Drug and alcohol testing.

* * * * *

(c) * * *

(3) Post-event. As soon as practical after an event involving a human error that was committed by an individual specified in § 26.4(f), where the human error may have caused or contributed to the event. The licensee or other entity shall test the individual(s) who committed the error(s), and need not test individuals who were affected by the event but whose actions likely did not cause or contribute to the event. The individual(s) who committed the human error(s) shall be tested if the event resulted in—

* * * * *

(f) Testing of urine and oral fluid specimens for drugs and validity must be performed in a laboratory that is certified by HHS for that purpose, consistent with its standards and procedures for certification. Specimens for initial validity or initial drug testing that yield positive, adulterated, substituted, or invalid test results must be subject to confirmatory testing by the HHS-certified laboratory, except for invalid specimens that cannot be tested. Testing of other specimens that yield positive initial drug test results must be subject to confirmatory testing by a laboratory that meets stringent quality control requirements that are comparable to those required for certification by the HHS.

(g) Licensees and other entities shall provide for an MRO review of positive, positive and dilute, adulterated, substituted, and invalid confirmatory drug and validity test results to determine whether the donor has violated the FFD policy, before reporting the results to the individual designated by the licensee or other entity to perform the suitability and fitness evaluations required under § 26.419.

37. Revise § 26.419 to read as follows:

§ 26.419 Suitability and fitness evaluations.

Licensees and other entities who implement FFD programs under this subpart shall develop, implement, and maintain procedures for evaluating whether to assign individuals to the duties specified in § 26.4(f). These procedures must provide reasonable assurance that the individuals are fit to safely and competently perform their duties, and are trustworthy and reliable, as demonstrated by the avoidance of substance abuse.

38. In § 26.606:

a. Revise paragraph (b)(6); and

b. Add paragraph (b)(7).

The revision and addition read as follows:

§ 26.606 Written policy and procedures

* * * * *

(b) * * *

(6) Measures to prevent subversion of drug and alcohol tests conducted onsite and offsite, and

(7) For licensees and other entities that allow escorting of individuals performing activities described in 10 CFR 26.4(f), but do not implement an FFD program under subpart K (or a program that meets all the requirements of part 26, except subpart M and subpart K) during construction, describe the process that the licensee or other entity

will use for the processing, escorting, and control of individuals under escort and the duties and responsibilities of escorts.

39. In § 26.607, add a last sentence to paragraph (b)(2)(vi) and revise paragraphs (c)(4) and (5) to read as follows:

§ 26.607 Drug and alcohol testing.

* * * * *

(b) * * *

(2) * * *

(vi) * * * In such instances, the consortium/third-party administrator must ensure that the testing rate for the random testing pool from which they sample meets the requirement in paragraph (b)(2)(v).

* * * * *

(c) * * *

(4) For all test conditions in paragraph (b) of this section and for MRO-directed tests under § 26.185, drug testing must be performed at an HHS-certified laboratory for the specific biological specimen to be tested. Only HHS-certified laboratory test results from urine and oral fluid specimens may be used for the issuance of a sanction required under this part.

(5) The licensee or other entity must establish and maintain a contract with an HHS-certified laboratory for each specimen to be tested. Each contract must stipulate the following:

(i) The laboratory must permit representatives of the NRC and any licensee or other entity using the laboratory's services to inspect or audit the laboratory at any time, including unannounced inspections;

(ii) Laboratory records and documents must be provided and/or able to be photocopied and removed from the premises to support the inspection or audit;

(iii) The laboratory must comply with the applicable provisions of any State licensor requirements;

(iv) The laboratory must make available qualified personnel to testify in an administrative or disciplinary proceeding against an individual when that proceeding is based on test results reported by the HHS-certified laboratory;

(v) The laboratory shall maintain test records in confidence, consistent with the requirements of § 26.37, and use them with the highest regard for individual privacy.

(vi) Consistent with the principles established in section 503 of Public Law 100 71, any employee of a licensee or other entity who is the subject of a drug test (or his or her representative designated under § 26.37(d)) must, on written request, have access to the laboratory's records related to his or her validity and drug test and any records related to the results of any relevant certification, review, or revocation-of-certification proceedings; and

(vii) The laboratory may not enter into any relationship with the licensee's or other entity's MRO(s) that may be construed as a potential conflict of interest, including, but not limited to, the relationships described in § 26.183(b), and may not derive any financial benefit by having a licensee or other entity use a specific MRO.

* * * * *

40. Revise § 26.715 to read as follows:

§ 26.715 Recordkeeping requirements for collection sites and laboratories certified by the Department of Health and Human Services.

(a) Collection sites providing services to licensees and other entities who are subject to this subpart and HHS-certified laboratories shall maintain and make available documentation of all aspects of the testing process for at least 2 years or until the completion of all legal proceedings related to a determination of an FFD violation, whichever is later. This 2-year period may be extended on written notification by the NRC or by any licensee or other entity for whom services are being provided.

(b) Documentation that must be retained includes, but is not limited to, the following:

(1) Personnel files, including training records, for all individuals who have been authorized to have access to specimens, but are no longer under contract to or employed by the collection site;

(2) Chain of custody documents (other than forms recording specimens with negative test results and no FFD violations or anomalies, which may be destroyed after appropriate summary information has been recorded for program administration purposes);

(3) Quality assurance and quality control records;

(4) Superseded procedures;

(5) All test data (including calibration curves and any calculations used in determining test results);

(6) Test reports;

(7) Records pertaining to performance testing;

(8) Records pertaining to the investigation of testing errors or unsatisfactory performance discovered in quality control or blind performance testing, in the testing of actual specimens, or through the processing of appeals and MRO reviews, as well as any other errors or matters that could adversely reflect on the integrity of the testing process, investigation findings, and corrective actions taken, where applicable;

(9) Performance records on certification inspections;

(10) Records that summarize any test results that the MRO determined to be scientifically insufficient for further action;

(11) Either printed or electronic copies of computer-generated data;

(12) Records that document the dates, times of entry and exit, escorts, and purposes of entry of authorized visitors, maintenance personnel, and service personnel who have accessed secured areas of HHS-certified laboratories; and

(13) Records of the inspection, maintenance, and calibration of EBTs.

41. In § 26.717:

a. In paragraph (b)(2) remove the word “dilute”;

b. Revise paragraphs (b)(7) and (8);

c. Remove paragraph (d); and

d. Redesignate paragraphs (e) through (g) as paragraphs (d) through (f).

The revisions to read as follows:

§ 26.717 Fitness-for-duty program performance data.

* * * * *

(b) * * *

(7) Number of subversion attempts by type; and

(8) Summary of management actions.

* * * * *

42. In § 26.719, revise the introductory text to paragraphs (b) and (b)(2), and revise paragraph (c) to read as follows:

§ 26.719 Reporting requirements.

* * * * *

(b) *Significant FFD policy violations or programmatic failures.* The following significant FFD policy violations and programmatic failures must be reported to the NRC Headquarters Operations Center by telephone within 24 hours after the licensee or other entity discovers the violation:

* * * * *

(2) Any acts by any person licensed under 10 CFR part 55 to operate a power reactor, as well as any acts by SSNM transporters, FFD program personnel, or any supervisory personnel directing the operation or maintenance of safety- or security-related SSCs or directing the performance of security duties under § 26.4(a)(5) who are authorized under this part, if such acts—

* * * * *

(c) *Drug and alcohol testing errors.*

(1) Within 30 days of completing an investigation of any testing errors or unsatisfactory performance discovered in performance testing at an HHS-certified laboratory, in the testing of quality control or actual specimens, or through the processing of reviews under § 26.39 and MRO reviews under § 26.185, as well as any other errors or matters that could adversely reflect on the integrity of the random selection or testing process, the licensee or other entity shall submit to the NRC a report of the incident and corrective actions taken or planned. If the error involves an HHS-certified laboratory, the NRC shall ensure that HHS is notified of the finding.

(2) If a false positive or false negative error occurs on a blind performance test sample submitted to an HHS-certified laboratory, the licensee or other entity shall notify the NRC within 24 hours after discovery of the error.

* * * * *

PART 50—DOMESTIC LICENSING OF PRODUCTION AND UTILIZATION FACILITIES

43. The authority citation for part 50 continues to read as follows:

Authority: Atomic Energy Act of 1954, secs. 11, 101, 102, 103, 104, 105, 108, 122, 147, 149, 161, 181, 182, 183, 184, 185, 186, 187, 189, 223, 234 (42 U.S.C. 2014, 2131, 2132, 2133, 2134, 2135, 2138, 2152, 2167, 2169, 2201, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2239, 2273, 2282); Energy Reorganization Act of 1974, secs. 201, 202, 206, 211 (42 U.S.C. 5841, 5842, 5846, 5851); Nuclear Waste Policy Act of 1982, sec. 306 (42 U.S.C. 10226); National Environmental Policy Act of 1969 (42 U.S.C. 4332); 44 U.S.C. 3504 note.

44. In § 50.34, revise paragraphs (a)(3)(i) and (ii), (c)(2), (d)(2), (e), and (f)(2)(xxviii) to read as follows:

§ 50.34 Contents of applications; technical information.

(a) * * *

(3) * * *

(i) The principal design criteria for the facility. Appendix A, General Design Criteria for Nuclear Power Plants, establishes minimum requirements for the principal design criteria for water-cooled nuclear power plants similar in design and location to plants for which construction permits have previously been issued by the Commission and provides guidance to applicants for construction permits in establishing principal design criteria for other types of nuclear power units. For each application for an operating license for a utilization facility submitted after [EFFECTIVE DATE], safety and security must be considered together in the design process such that, where possible, security issues are effectively resolved through design and engineered security features;

(ii) The design bases and the relation of the design bases to the principal design criteria; and

* * * * *

(c) * * *

(2) Each applicant for an operating license for a utilization facility that will be subject to the requirements of § 73.55 or § 73.100 of this chapter must include a physical security plan, a training and qualification plan in accordance with the criteria set forth in appendix B to part 73 of this chapter or § 73.100 of this chapter, and a cybersecurity plan in accordance with the criteria set forth in § 73.54 or § 73.110 of this chapter.

(d) * * *

(2) Each application for a license to operate a utilization facility that will be subject to § 73.55 or § 73.100 of this chapter must include a licensee safeguards contingency plan in accordance with the criteria set forth in section II of appendix C to part 73 of this chapter. The “implementing procedures” required in section II of appendix C to part 73 of this chapter do not have to be submitted to the Commission for approval.

* * * * *

(e) Protection against unauthorized disclosure. Each applicant for an operating license for a production or utilization facility, who prepares a physical security plan, a

safeguards contingency plan, a training and qualification plan, or a cybersecurity plan, shall protect the plans and other related Safeguards Information against unauthorized disclosure in accordance with the requirements of § 73.21 of this chapter.

(f) * * *

(2) * * *

(xxviii) Evaluate potential pathways for radioactivity and radiation that may lead to control room habitability problems under accident conditions resulting in an accident source term[6] release and make necessary design provisions to preclude such problems. (III.D.3.4)

* * * * *

PART 52—LICENSES, CERTIFICATIONS, AND APPROVALS FOR NUCLEAR POWER PLANTS

45. The authority citation for part 52 is revised to read as follows:

Authority: Atomic Energy Act of 1954, secs. 103, 104, 147, 149, 161, 181, 182, 183, 185, 186, 189, 223, 234 (42 U.S.C. 2133, 2134, 2167, 2169, 2201, 2231, 2232, 2233, 2235, 2236, 2239, 2273, 2282); Energy Reorganization Act of 1974, secs. 201, 202, 206, 211 (42 U.S.C. 5841, 5842, 5846, 5851); 44 U.S.C. 3504 note.

46. In § 52.79:

a. Revise paragraphs (a)(4)(i) and (ii) and (a)(36)(ii) through (v); and

b. In footnote 8, add the phrase “or § 73.100” after the phrase “§ 75.55”.

The revisions read as follows:

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

(a) * * *

(4) * * *

(i) The principal design criteria for the facility. Appendix A to part 50 of this chapter, “General Design Criteria for Nuclear Power Plants,” establishes minimum requirements for the principal design criteria for water-cooled nuclear power plants

similar in design and location to plants for which construction permits have previously been issued by the Commission and provides guidance to applicants in establishing principal design criteria for other types of nuclear power units. For each application for a combined license submitted after [EFFECTIVE DATE], safety and security must be considered together in the design process such that, where possible, security issues are effectively resolved through design and engineered security features;

(ii) The design bases and the relation of the design bases to the principal design criteria; and

* * * * *

(36) * * *

(ii) A training and qualification plan in accordance with the criteria set forth in appendix B to 10 CFR part 73 or § 73.100 of this chapter;

(iii) A cybersecurity plan in accordance with the criteria set forth in § 73.54 or § 73.110 of this chapter;

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

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

* * * * *

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

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

Authority: Atomic Energy Act of 1954, secs. 51, 53, 57, 62, 63, 65, 69, 81, 161, 182, 183, 184, 186, 187, 189, 223, 234, 274 (42 U.S.C. 2071, 2073, 2077, 2092, 2093, 2095, 2099, 2111, 2201, 2210e, 2232, 2233, 2234, 2236, 2237, 2238, 2273, 2282,

2021); Energy Reorganization Act of 1974, secs. 201, 202, 206, 211 (42 U.S.C. 5841, 5842, 5846, 5851); National Environmental Policy Act of 1969 (42 U.S.C. 4332); Nuclear Waste Policy Act of 1982, secs. 117(a), 132, 133, 134, 135, 137, 141, 145(g), 148, 218(a) (42 U.S.C. 10137(a), 10152, 10153, 10154, 10155, 10157, 10161, 10165(g), 10168, 10198(a)); 44 U.S.C. 3504 note.

48. In § 72.13, add paragraph (e) to read as follows:

§ 72.13 Applicability

* * * * *

(e) The following sections apply to activities associated with a general license, where the licensee has elected to provide for physical protection of the spent fuel in accordance with § 72.212(b)(9)(iv): § 72.1; § 72.2(a)(1), (b), (c), and (e); §§ 72.3 through 72.6(c)(1); §§ 72.7 through § 72.13(a) and (e); § 72.30(b), (c), (d), (e), and (f); § 72.32(c) and (d); § 72.44(b) and (f); § 72.48; § 72.50(a); § 72.52(a), (b), (d), and (e); § 72.60; § 72.62; §§ 72.72 through 72.80(f); §§ 72.82 through 72.86; §§ 72.104 through 72.106; §§ 72.122 through 72.126; §§ 72.140 through 72.176; §§ 72.180 through 72.186; § 72.190; § 72.194; §§ 72.210 through 72.220; and § 72.240(a).

§ 72.32 [Amended]

49. In § 72.32, in paragraphs (a)(8) and (b)(8), remove the phrase “NRC operations center” and add in its place the phrase “NRC Headquarters Operations Center”.

§ 72.44 [Amended]

50. In § 72.44, in the last sentence of paragraph (e), remove the time period “two months” and add in its place the phrase “12 months”.

§ 72.186 [Amended]

51. In § 72.186, in the second sentence of paragraph (b), remove the time period “two months” and add in its place the phrase “12 months”.

52. In § 72.212, revise paragraph (b)(9) to read as follows:

§ 72.212 Conditions of general license issued under § 72.210.

* * * * *

(b) * * *

(9) Protect the spent fuel against the design basis threat of radiological sabotage in accordance with the same provisions and requirements as are set forth in the licensee's physical security plan pursuant to § 73.55 of this chapter with the following additional conditions and exceptions:

(i) The physical security organization and program for the facility must be modified as necessary to assure that activities conducted under this general license do not decrease the effectiveness of the protection of vital equipment in accordance with § 73.55 of this chapter;

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

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

(iv)(A) When a separate protected area is established outside of an existing protected area for the purpose of storage of spent fuel, the licensee may, as an alternative to the requirements of § 72.212(b)(9)(i) and (b)(9)(ii), provide for the physical protection of the spent fuel under subpart H of this part and § 73.51 of this chapter;

(B) Upon NRC docketing of the certifications required under § 50.82(a)(1) of this chapter or § 52.110(a) of this chapter or § 53.1070(a) of this chapter, and when all spent fuel has been placed in dry cask storage at the facility, the licensee may, as an alternative to the requirements of § 72.212(b)(9)(i) and (b)(9)(ii), provide for physical protection of the spent fuel under subpart H of this part and § 73.51 of this chapter;

(C) A licensee who elects to provide physical protection under subpart H of this part and § 73.51 of this chapter must submit their physical security plan to the NRC under § 50.54(p) of this chapter; and

(v) Each general licensee that receives and possesses power reactor spent fuel and other radioactive materials associated with spent fuel storage shall protect Safeguards Information against unauthorized disclosure in accordance with the requirements of § 73.21 and the requirements of § 73.22 or § 73.23 of this chapter, as applicable.

* * * * *

PART 73—PHYSICAL PROTECTION OF PLANTS AND MATERIALS

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

Authority: Atomic Energy Act of 1954, secs. 53, 147, 149, 161, 161A, 170D, 170E, 170H, 170I, 223, 229, 234, 1701 (42 U.S.C. 2073, 2167, 2169, 2201, 2201a, 2210d, 2210e, 2210h, 2210i, 2273, 2278a, 2282, 2297f); Energy Reorganization Act of 1974, secs. 201, 202 (42 U.S.C. 5841, 5842); Nuclear Waste Policy Act of 1982, secs. 135, 141 (42 U.S.C. 10155, 10161); 44 U.S.C. 3504 note.

Section 73.37(b)(2) also issued under Sec. 301, Public Law 96-295, 94 Stat. 789 (42 U.S.C. 5841 note).

54. In part 73, wherever it may appear, the term or phrase in the left column in the following table is removed and the term or phrase in the right column is added in its place.

Remove	Add
cyber attacks	cyberattacks
cyber security	cybersecurity
Division of Physical and Cyber Security Policy	Division of Physical and Cybersecurity Policy
NRC Operations Center	NRC Headquarters Operations Center

55. In § 73.2:

a. Revise the definitions of "*Contraband*", "*DOE* and *Department of Energy*", "*Physical barrier*", and "*Security Storage Container*"; and

b. Add, in alphabetical order, the definition for "*Target set*" to read as follows:

§ 73.2 Definitions.

* * * * *

Contraband means unauthorized firearms, explosives, incendiary devices, or other items that may be carried or concealed by personnel, packages, materials, or vehicles and could be used to commit radiological sabotage.

* * * * *

DOE and *Department of Energy* means the Department of Energy established by the Department of Energy Organization Act (Pub. L. 95-91, 91 Stat. 565, 42 U.S.C. 7101 *et seq.*), to the extent that the Department, or its duly authorized representatives, exercises functions formerly vested in the U.S. Atomic Energy Commission, its Chairman, members, officers and components and transferred to the U.S. Energy Research and Development Administration and to the Administrator thereof pursuant to sections 104(b), (c) and (d) of the Energy Reorganization Act of 1974 (Pub. L. 93-438, 88 Stat. 1233 at 1237, 42 U.S.C. 5814) and retransferred to the Secretary of Energy pursuant to section 301(a) of the Department of Energy Organization Act (Pub. L. 95-91, 91 Stat. 565 at 577-578, 42 U.S.C. 7151).

* * * * *

Physical barrier means:

(1) Fencing composed of durable wire fabric, topped by barbed wire or similar material on brackets, with an overall height sufficient to achieve the purpose for which the barrier is intended, as determined by a site-specific analysis;

(2) Building walls, ceilings and floors constructed of stone, brick, cinder block, concrete, steel or comparable materials (openings in which are secured by grates, doors, or covers of construction and fastening of sufficient strength such that the integrity of the wall is not lessened by any opening), or walls of similar construction, not part of a

building, provided with a barbed or similar material topping as described in paragraph (1), and of a height as described in paragraph (1).

(3) Any other physical obstruction constructed in a manner and of materials suitable for the purpose for which the obstruction is intended that is considered equivalent to paragraphs (1) and (2).

* * * * *

Security Storage Container includes any of the following repositories: (1) For storage in a building located within a protected or controlled access area, a steel filing cabinet equipped with a steel locking bar and a three position, changeable combination, GSA approved padlock; (2) A security filing cabinet that bears a Test Certification Label on the side of the locking drawer, or interior plate, and is marked, *General Services Administration Approved Security Container* on the exterior of the top drawer or door; (3) A bank safe-deposit box; and (4) Other repositories which in the judgment of the NRC, would provide comparable physical protection.

* * * * *

Target set means the minimum combination of equipment, operator actions, or structures, which, if all are prevented from performing their intended function or prevented from being accomplished, barring extraordinary actions by plant operations, would likely result in a release of radionuclides from any source that would exceed the dose reference values defined in § 50.34(a)(1)(ii)(D)(*1*) and (*2*) of this chapter, § 52.79(a)(1)(vi)(A) and (B) of this chapter, or § 53.210 of this chapter, as applicable.

* * * * *

§ 73.8 [Amended]

56. In § 73.8, in paragraph (b), remove the reference “73.58,”.

57. In § 73.15:

a. In paragraphs (e)(6) and (r)(1) and (2), remove the phrase “§ 50.90, § 70.34, or § 72.56 of this chapter” and add in its place the phrase “§ 50.90, § 53.1510, § 70.34, or § 72.56 of this chapter”; and

b. Revise paragraphs (b)(2) and (s)(3) and the introductory text of paragraph (s)(4) to read as follows:

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

* * * * *

(b) * * *

(2) With respect to the possession and use of firearms by all other NRC licensees, the Commission’s requirements in effect before April 13, 2023, remain applicable, except to the extent that those requirements are modified by an NRC order or regulations applicable to these licensees.

* * * * *

(s) * * *

(3) Licensees must have completed their transition from the confirmatory orders to the requirements of this rule by January 8, 2024.

(4) Effective January 8, 2024, the following orders were withdrawn:

* * * * *

§ 73.17 [Amended]

58. In § 73.17:

a. In paragraph (b)(4)(ii), remove the word “personal” and add in its place the word “personnel”; and

b. In paragraph (r), add a comma after the date “April 13, 2023”.

59. In § 73.20, revise paragraph (a) to read as follows:

§ 73.20 General performance objective and requirements.

(a) In addition to any other requirements of this part, each licensee who is authorized to operate a spent fuel reprocessing plant pursuant to part 50 or part 70 of this chapter; possesses or uses formula quantities of strategic special nuclear material at any site or contiguous sites subject to control by the licensee; is authorized to transport or deliver to a carrier for transportation pursuant to part 70 of this chapter formula quantities of strategic special nuclear material; takes delivery of formula quantities of strategic special nuclear material free on board (f.o.b.) the point at which it is delivered to a carrier for transportation; or imports or exports formula quantities of strategic special nuclear material, shall establish and maintain or make arrangements for a physical protection system which will have as its objective to provide reasonable assurance that activities involving special nuclear material are not inimical to the common defense and security, and do not constitute an unreasonable risk to the public health and safety. The physical protection system shall be designed to protect against the design basis threats of theft or diversion of strategic special nuclear material and radiological sabotage as stated in § 73.1(a).

* * * * *

60. In § 73.22, revise paragraph (f)(3) and (g) to read as follows:

§ 73.22 Protection of Safeguards Information: Specific requirements.

* * * * *

(f) * * *

(3) Except under emergency or extraordinary conditions, Safeguards Information shall be transmitted outside an authorized place of use or storage only by encrypted means, provided that transmitters and receivers implement processes that will provide reasonable assurance that Safeguards Information is protected before and after the transmission or electronic mail through the internet. Digital voice communication of Safeguards Information shall utilize a commercially available encryption system that is compliant with an active, approved version of Federal Information Processing Standard

(FIPS) 140. Documents containing Safeguards Information shall be processed on a self-contained secure computer system and only transferred to a networked system for transmission once it has been appropriately encrypted. The recipient shall only decrypt the Safeguards Information on a self-contained computer system. Symmetric keys or passwords for encrypted Safeguards Information shall be transmitted to the recipient by a means other than that used to transmit the encrypted data. Physical or cybersecurity events required to be reported pursuant to the reporting requirements in this part are considered to be extraordinary conditions.

(g) Processing of Safeguards Information on electronic systems.

(1) Safeguards Information may be stored, processed or produced on a stand-alone computer (or computer system) for processing of Safeguards Information. “Stand-alone” means a computer or computer system to which access is limited to individuals authorized access to Safeguards Information. A stand-alone computer or computer system shall not be physically or in any other way connected to a network accessible by users who are not authorized access to Safeguards Information.

(i) Each computer not located within an approved and lockable security storage container that is used to process Safeguards Information must have a removable storage medium with a bootable operating system. The bootable operating system must be used to load and initialize the computer. The removable storage medium must also contain the software application programs. Data may be saved on either the removable storage medium that is used to boot the operating system, or on a different removable storage medium. The removable storage medium must be secured in a locked security storage container when not in use.

(ii) A mobile device (such as a laptop computer) may also be used for the processing of Safeguards Information provided the device is secured in a locked security storage container when not in use. Other systems may be used if approved for security by the appropriate NRC office.

(iii) Any electronic system that has been used for storage, processing or production of Safeguards Information must be free of recoverable Safeguards Information prior to being returned to nonexclusive use.

(2) As an alternative to paragraph (g)(1) of this section, Safeguards Information may be stored, processed or produced on a computer or computer system and viewed through a network connection, provided that the computer or computer system used to store the Safeguards Information is stored in a security storage container and information security controls are implemented that ensure the Safeguards Information is accessible only by individuals authorized access to Safeguards Information.

(i) Authorized users may access the Safeguards Information using a thin client, virtual desktop, or similar architecture that ensures the Safeguards Information cannot be intentionally or inadvertently transferred or stored on computers not authorized to store the information.

(ii) Computers or servers used to implement this alternative shall be physically located within a security storage container.

(iii) Computers or servers used to implement this alternative shall be protected by the cybersecurity controls described in an active and approved version of National Institute of Standards and Technology (NIST) Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

(iv) Persons implementing this alternative shall describe in processes, procedures, and other records how the security controls in NIST SP 800-171 are implemented.

* * * * *

61. In § 73.23, revise paragraph (f)(3) and in paragraph (g)(2), remove the phrase “to Federal Information Processing Standards (FIPS) 140-2 or later” and add in its place the phrase “to an active, approved version of the Federal Information Processing Standards (FIPS) 140 standard”.

The revision to read as follows:

§ 73.23 Protection of Safeguards Information—Modified Handling: Specific requirements.

* * * * *

(f) * * *

(3) Except under emergency or extraordinary conditions, Safeguards Information designated as Safeguards Information-Modified Handling must be transmitted electronically only by protected telecommunications circuits (including facsimile) that utilizes a commercially available encryption system that is compliant with an active, approved version of Federal Information Processing Standard (FIPS) 140. For the purpose of this section, emergency or extraordinary conditions are defined as any circumstances that require immediate communications in order to report, summon assistance for, or respond to a security contingency event or an event that has potential security significance. Physical security events required to be reported pursuant to §§ 73.1200 and 73.1205 are considered to be extraordinary conditions.

* * * * *

62. In § 73.46:

a. Revise paragraph (b).

b. In paragraph (h)(3) remove the word “availabiliy” and add in its place the word “availability”; and

c. Remove paragraph (i).

The revision reads as follows:

§ 73.46 Fixed site physical protection systems, subsystems, components, and procedures.

*** * * * ***

(b) Security organization.

(1) The licensee shall establish a security organization, including guards. If a contract guard force is utilized for site security, the licensee’s written agreement with the

contractor will clearly show that (i) the licensee is responsible to the Commission for maintaining safeguards in accordance with Commission regulations and the licensee's security plan, (ii) the NRC may inspect, copy, and take away copies of all reports and documents required to be kept by Commission regulations, orders, or applicable license conditions whether such reports and documents are kept by the licensee or the contractor, (iii) the requirement, in § 73.46(b)(4) of this section that the licensee demonstrate the ability of physical security personnel to perform their assigned duties and responsibilities, include demonstration of the ability of the contractor's physical security personnel to perform their assigned duties and responsibilities in carrying out the provisions of the Security Plan and these regulations, and (iv) the contractor will not assign any personnel to the site who have not first been made aware of these responsibilities.

(2) The licensee shall have onsite at all times at least one full time member of the security organization with authority to direct the physical protection activities of the security organization.

(3) The licensee shall have a management system to provide for the development, revision, implementation, and enforcement of security procedures. The system shall include:

(i) Written security procedures which document the structure of the security organization and which detail the duties of the Tactical Response Team, guards, watchmen, and other individuals responsible for security. The licensee shall retain a copy of the current procedures as a record until the Commission terminates the license for which these procedures were developed and, if any portion of these procedures is superseded, retain the superseded material for three years after each change; and

(ii) Provision for written approval of such procedures and any revisions thereto by the individual with overall responsibility for the security function.

(4) The licensee may not permit an individual to act as a Tactical Response Team member, armed response person, guard, or other member of the security

organization unless the individual has been trained, equipped, and qualified to perform each assigned security duty in accordance with the licensee security plans and appendix B of this part, “General Criteria for Security Personnel.” In addition, Tactical Response Team members, armed response personnel, and guards shall be trained, equipped, and qualified for use of their assigned weapons in accordance with paragraphs (b)(6) and (b)(7) of this section. Tactical Response Team members, armed response personnel, and guards shall also be trained and qualified in accordance with paragraph (b)(10) of this section. Upon the request of an authorized representative of the Commission, the licensee shall demonstrate the ability of the physical security personnel, whether licensee or contractor employees, to carry out their assigned duties and responsibilities. Each Tactical Response Team member, armed response person, and guard, whether a licensee or contractor employee, shall requalify in accordance with appendix B of this part. Tactical Response Team members, armed response personnel, and guards shall also requalify in accordance with paragraph (b)(7) of this section at least once every 12 months. The licensee shall document the results of the qualification and requalification. The licensee shall retain the documentation of each qualification and requalification as a record for 3 years after each qualification and requalification.

(5) 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.

(6) Each guard shall be armed with a handgun, as described in appendix B of this part. Each Tactical Response Team member shall be armed with a 9-mm semiautomatic pistol. All but one member of the Tactical Response Team shall be armed additionally with either a shotgun or semiautomatic rifle, as described in appendix B of this part. The remaining member of the Tactical Response Team shall carry, as an individually assigned weapon, a rifle of no less caliber than .30 inches or 7.62 mm.

(7) In addition to the weapons qualification and requalification criteria of appendix B of this part, Tactical Response Team members, armed response personnel, and guards shall qualify and requalify, at least every 12 months, for day and night firing with assigned weapons in accordance with appendix H of this part. Tactical Response Team members, armed response personnel, and guards shall be permitted to practice fire prior to qualification and requalification but shall be given only one opportunity to fire for record on the same calendar day. If a Tactical Response Team member, armed response person, or guard fails to qualify or requalify, the licensee shall remove the individual from security duties which require the use of firearms and retrain the individual prior to any subsequent attempt to qualify or requalify. If an individual fails to qualify or requalify on two successive attempts, he or she shall be required to receive additional training and successfully fire two consecutive qualifying scores prior to being reassigned to armed security duties.

(i) In addition, Tactical Response Team members, armed response personnel, and guards shall be prepared to demonstrate day and night firing qualification with their assigned weapons at any time upon request by an authorized representative of the NRC.

(ii) The licensee or the licensee’s agent shall document the results of weapons qualification and requalification for day and night firing. The licensee shall retain the documentation of each qualification and requalification as a record for 3 years after each qualification and requalification.

(8) In addition to the training requirements contained in appendix B of this part, Tactical Response Team members shall successfully complete training in response tactics. The licensee shall document the completion of training. The licensee shall retain the documentation of training as a record for three years after training is completed.

(9) The licensee shall conduct Tactical Response Team and guard exercises to demonstrate the overall security system effectiveness and the ability of the security force to perform response and contingency plan responsibilities and to demonstrate individual

skills in assigned team duties. The licensee shall use these exercises to demonstrate its capability to respond to attempts of theft or diversion of strategic special nuclear material. On an annual basis, each shift that implements the safeguards contingency plan and licensee protective strategy must participate in two tactical response drills, one of which must test security response using the minimum necessary response force and a mock adversary team to execute the scenario. Every 3 years, each shift that implements the safeguards contingency plan and licensee protective strategy must participate in one force-on-force exercise. The licensee must conduct at least one force-on-force exercise annually. Force-on-force exercises conducted to satisfy the NRC triennial evaluation requirement can be used to satisfy the annual force-on-force requirement for the personnel that participate in the capacity of the security response organization. The licensee shall document the results of all exercises. The licensee shall retain the documentation of each exercise as a record for three years after each exercise is completed.

(10) In addition to the medical examinations and physical fitness requirements of paragraph I.C of appendix B of this part, each Tactical Response Team member, armed response person, and guard, except as provided in paragraph (b)(10)(v) of this section, shall participate in a physical fitness training program, to include a physical fitness test, on an initial and continuing basis.

(i) The licensee must administer a physical fitness test to all Tactical Response Team members, armed response personnel, and guards once every 6 months. Individuals who exceed 6 months without having been administered the test due to excused time off from work must be tested within 15 calendar days of returning to duty as a Tactical Response Team member, armed response person, or guard.

(ii) The physical fitness test must address the physical capabilities needed by armed response personnel during strenuous tactical engagements, and include physical exertion, levels of stress, and exposure to the elements as they pertain to each individual’s assigned security duties for both normal and emergency operations. The test

must simulate site specific conditions under which the individual will be required to perform assigned duties and responsibilities.

(iii) The licensee shall give Tactical Response Team members, armed response personnel, and guards a medical examination including a determination and written certification by a licensed physician that there are no medical contraindications, as disclosed by the medical examination, to participate in the physical fitness test. The medical examination must be given within 30 days prior to the first administration of the physical fitness test, and on an annual basis thereafter.

(iv) Licensees may temporarily waive an individual's participation in the physical fitness test on the advice of the licensee's examining physician, during which time the individual may not be assigned duties as a Tactical Response Team member, armed response person, or guard.

(v) Guards whose duties are to staff the central or secondary alarm station and those who control exit or entry portals are exempt from the physical fitness training program specified in paragraph (b)(10) of this section, provided that they are not assigned temporary response guard duties.

(vi) The licensee shall place Tactical Response Team members, armed response persons, and guards, who do not meet the licensee-established qualification criteria, in a monitored remedial physical fitness training program and relieve them of security duties until they satisfactorily meet the licensee-established qualification criteria.

63. In § 73.51:

a. Revise paragraphs (a) and (b)(1);

b. In paragraph (d)(1), remove the phrase ", typically 20 feet wide each, on both sides of this barrier,";

c. In paragraph (d)(3), in the last sentence, remove the word "redundant" and add in its place the word "additional";

d. In paragraph (d)(11), remove the phrase "of the" in the last sentence; and

e. In paragraph (d)(12), in the first sentence, remove the number “24” and add in its place the number “36”.

The revisions read as follows:

§ 73.51 Requirements for the 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:

(1) Under a specific license issued pursuant to part 72 of this chapter:

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

(ii) At a monitored retrievable storage (MRS) installation; or

(2) At a geologic repository operations area (GROA) licensed pursuant to part 60 or 63 of this chapter; or

(3) Under a general license issued pursuant to part 72 of this chapter:

(i) When a separate protected area is established outside of an existing protected area for the purpose of storage of spent fuel and a submittal has been made to the NRC under the provisions of § 72.212(b)(9)(iv)(C) of this chapter; or

(ii) Upon the NRC’s docketing of the certifications required under § 50.82(a)(1) of this chapter or § 52.110(a) of this chapter or § 53.1070(a) of this chapter, when all spent fuel has been placed in dry cask storage at the facility, and a submittal has been made to the NRC under the provisions of § 72.212(b)(9)(iv)(C) of this chapter.

(b) * * *

(1) Each licensee subject to this section shall establish and maintain a physical protection system with the objective of providing reasonable assurance that activities involving spent nuclear fuel and high-level radioactive waste do not constitute an unreasonable risk to public health and safety.

* * * * *

64. Revise § 73.54 to read as follows:

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

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

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

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

(ii) Security functions;

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

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

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

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

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

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

(b) To accomplish this, the licensee shall:

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

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

(3) [Reserved]

(c) The cybersecurity program must be designed to:

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

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

(3) Mitigate the adverse effects of cyberattacks; and

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

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

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

(2) Evaluate and manage cyber risks.

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

(4) Conduct cybersecurity event notifications in accordance with the provisions of § 73.77.

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

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

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

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

(ii) Mitigate the consequences of cyberattacks;

(iii) Correct exploited vulnerabilities; and

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

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

(g) The licensee must establish and implement cybersecurity reviews to assess the effectiveness of the implementation of the cybersecurity program.

(1) The licensee must review each element of the cybersecurity program at a frequency commensurate with the importance or significance to safety of plant operations to ensure timely identification and documentation of vulnerabilities, improvements, and corrective actions.

(2) Cybersecurity reviews must be performed by individuals independent of those personnel responsible for program management and any individual who has direct responsibility for implementing the cybersecurity program.

(3) The licensee must establish and perform self-assessments to ensure the effective implementation of the cybersecurity program.

(4) The results and recommendations of the cybersecurity program reviews, management’s findings regarding program effectiveness, and any actions taken as a result of recommendations from prior program reviews, must be documented in a report and must be maintained in an auditable form and available for inspection.

(h) The licensee shall retain all records and supporting technical documentation required to satisfy the requirements of this section as a record until the Commission terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified by the Commission.

65. Revise § 73.55 to read as follows:

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

(a) *Introduction.*

(1) Each licensee that is licensed to operate a nuclear power plant under 10 CFR part 50 and each holder of a combined license under 10 CFR part 52 must identify achievable target sets in accordance with § 73.55(f) and develop, implement, and maintain a physical protection program under the following requirements:

(i) Each licensee that demonstrates no achievable target sets exist in accordance with § 73.55(f), and does not credit any active measures (e.g., operator action, mitigative action, detection, assessment, armed response) in making that demonstration, is exempt from the remaining requirements of this section. The requirements of 10 CFR part 26, 10 CFR part 37, and §§ 73.21, 73.22, 73.23, 73.54, 73.67, 73.110, and 73.120 must be implemented as applicable.

(ii) Each licensee that demonstrates no achievable target sets exist in accordance with § 73.55(f), and credits active measures in making that demonstration, must implement the requirements of this section through its physical security plan, training and qualification plan, safeguards contingency plan, and cybersecurity plan, referred to collectively hereafter as ‘‘security plans,” before initial fuel load into the reactor (or, for a fueled manufactured reactor, before initiating the removal of features to prevent criticality); for such licensees, the requirements of § 73.55(b)(2) and (b)(3) shall be deemed satisfied if the physical protection program is designed to ensure that the credited active measures will be implemented in response to threats up to and including the design basis threat of radiological sabotage or,

(iii) Each licensee that demonstrates achievable target sets exist, in accordance with § 73.55(f), must implement the requirements of this section through its physical security plan, training and qualification plan, safeguards contingency plan, and cybersecurity plan, referred to collectively hereafter as ‘‘security plans,” before initial fuel

load into the reactor (or, for a fueled manufactured reactor, before initiating the removal of the features to prevent criticality).

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

(i) The security plans must describe how the performance objective and requirements set forth in this section will be implemented.

(ii) The licensee must protect the security plans and other security-related information against unauthorized disclosure in accordance with the requirements of § 73.21.

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

(b) *General performance objective and requirements*.

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

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

(3) The physical protection program must be designed to prevent a release of radionuclides from any source that exceeds the dose reference values defined in § 50.34(a)(1)(ii)(D)(*1*) and (*2*), § 52.79(a)(1)(vi)(A) and (B), or § 53.210 of this chapter, as applicable. Specifically, the program must:

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

(ii) Provide defense in depth in achieving performance requirements through the integration of engineered systems, technologies, administrative controls, implementing procedures and management measures as needed to ensure the effectiveness of the physical protection program.

(iii) For licensee physical protection programs that rely upon design and engineered security features to meet the requirements of this section, ensure that the reliability and availability of the structures, systems, and components (SSCs) for demonstrating compliance are maintained at all times.

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

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

(i) For licensees that rely upon SSCs in accordance with paragraph (b)(3)(iii) of this section, the performance evaluations must include methods appropriate and necessary to assess, test, and challenge the integration of the physical protection program’s functions to protect against the design basis threat, including measures to protect against cyberattack and engineered systems designed to protect against the design basis threat standalone ground vehicle bomb attack.

(A) The licensee must establish the frequencies for performance evaluations of the engineered security features commensurate with their security significance to the physical protection program.

(B) The licensee must document processes and procedures for implementing the performance evaluations. The licensee must maintain records, including results, findings, and corrective actions identified during the performance evaluations.

(ii) [Reserved]

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

(7) The licensee must establish, maintain, and implement a cybersecurity program in accordance with § 73.54 or § 73.110 and must describe the program in the cybersecurity plan.

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

(i) The insider mitigation program must monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorization to a protected or vital area, and implement defense-in-depth methodologies to minimize the potential for an insider (active, passive, or both) to adversely affect, either directly or indirectly, the licensee's capability to protect against the design basis threat of radiological sabotage as described in 10 CFR 73.55(b)(3).

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

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

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

(C) The cybersecurity program described in § 73.54 or § 73.110; and

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

(9) The licensee must track, trend, correct and prevent recurrence of failures and deficiencies in the implementation of the requirements of this section.

(10) Implementation of security plans and associated procedures must be coordinated with other onsite plans and procedures to preclude conflict during both normal and emergency conditions and ensure the adequate management of the safety and security interface.

(11)(i) The licensee must ensure that the firearms background check requirements of § 73.17 are met for all members of the security organization whose official duties require access to covered weapons or who inventory enhanced weapons.

(ii) The provisions of this paragraph are only applicable to licensees subject to this section that are also subject to the firearms background check provisions of § 73.17.

(c) *Security implementing procedures*.

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

(i) Implementing procedures must document the conduct of security operations, maintenance, training and qualification, contingency responses, and as applicable security design and configuration controls.

(ii) The revisions to security implementing procedures must satisfy the requirements of this section.

(2) [Reserved]

(d) *Security organization*.

(1) The licensee must establish and maintain a security organization that is staffed, trained, qualified, and equipped to implement the physical protection program under the requirements of this section, section VI of appendix B of this part, and the security plans.

(2) The security organization must include at least one member, onsite and available at all times, who has the authority to direct the activities of the security organization and who is assigned no other duties that would interfere with this

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

(3) As applicable, the licensee must—

(i) Establish a process for the approval of designs, policies, processes, and procedures and changes by the individual with overall responsibility for the physical protection program; and

(ii) Ensure that revisions and changes to the physical protection program and implementing policies, processes, and procedures satisfy the requirements of this section.

(e) *Physical barriers*.

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

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

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

(4) Protected area.

(i) The protected area perimeter must be protected by physical barriers that are designed and constructed to limit access into the protected area to only those personnel, vehicles, and materials required to perform official duties.

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

(5) Vital areas.

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

(ii) At a minimum, the following must be considered vital areas, as applicable:

(A) The reactor control room;

(B) The spent fuel pool; and

(C) The central alarm station.

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

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

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

(6) Land and waterborne vehicle control measures. Consistent with the physical protection program design requirements of § 73.55(b), and in accordance with the site-specific analysis, the licensee must establish and maintain as applicable, land and waterborne vehicle control measures, as necessary, to protect against the design basis threat of radiological sabotage land and waterborne vehicle bomb assaults.

(i) Licensee must provide periodic surveillance and observation of land and waterborne vehicle barrier systems adequate to detect indications of tampering and degradation or to otherwise ensure that each vehicle barrier and barrier system is able to satisfy the intended function.

(ii) [Reserved]

(f) *Target sets*.

(1) The licensee must identify complete and accurate target sets. Preventative operator actions may be credited as target set elements when: sufficient time to implement exists; environmental conditions allow operator actions to be completed successfully; adversary interference is precluded; all equipment required for operator actions is available, dedicated, staged, and maintained; approved procedures exist

specific to the task being performed; and training is maintained for proficiency of the credited operator action.

(2) The identification of target sets must not assume the success of the security organization; except that licensees may consider delay provided by the security organization when assessing the availability of operator actions.

(3) The licensee must consider cyberattacks in the identification of target sets.

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

(5) The licensee must document and maintain the process used to identify achievable target sets, to include the site-specific analyses and methodologies used to determine and group the target set equipment or elements, including elements not contained in a protected or vital area.

(6) The licensee must further identify achievable target sets through site-specific analyses. Achievable target sets are described by the following conditions:

(i) Are within the capabilities of the design basis threat adversary to compromise, destroy, or render non-functional;

(ii) Cannot be mitigated after adversary interference is precluded and prior to a release of radionuclides exceeding dose reference values defined in § 50.34(a)(1)(ii)(D)(*1*) and (*2*), § 52.79(a)(1)(vi)(A) and (B), or § 53.210 of this chapter, as applicable.

(iii) If defeated, result irreversibly in exceedance of the dose reference values defined in § 50.34(a)(1)(ii)(D)(*1*) and (*2*), § 52.79(a)(1)(vi)(A) and (B), or § 53.210 of this chapter, as applicable.

(7) The licensee must implement a process for the oversight of target set equipment and systems to ensure that changes to the configuration of the identified

equipment and systems are considered in the licensee's protective strategy. Where appropriate, changes must be made to documented target sets.

(8) The licensee must maintain the site-specific analyses for achievable target sets as a record in accordance with paragraph (q) of this section.

(g) *Access controls*.

(1) Barriers.

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

(ii) As applicable, the licensee must assign an individual the responsibility for the last access control function (controlling admission to the protected area) in accordance with § 73.55(e)(3).

(2) Protected areas.

(i) Before granting access into the protected area, the licensee must:

(A) Confirm the true identity of individuals.

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

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

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

(ii) [Reserved]

(3) Vehicles in the protected area.

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

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

(4) Vital areas.

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

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

(5) Emergency or exigent conditions.

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

(ii) In instances where licensees need to manage exigent circumstances, licensees can permit access in accordance with paragraphs (g)(7) and (8) of this section.

(6) Access control devices.

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

(ii) The licensee must implement a personnel identification system for all individuals authorized unescorted access to the protected area and vital areas.

(7) Visitors.

(i) The licensee may permit escorted access to protected and vital areas to individuals who have not been granted unescorted access in accordance with the requirements of § 73.56 and part 26 of this chapter. The licensee must:

(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.

(ii) Individuals not employed by the licensee but who require frequent or extended unescorted access to the protected area and/or vital areas to perform duties

and responsibilities required by the licensee at irregular or intermittent intervals, must satisfy the access authorization requirements of § 73.56 and part 26 of this chapter.

(8) Escorts.

(i) The licensee must ensure that all escorts are trained to perform escort duties and provided a means of timely communication with security personnel to summon assistance when needed.

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

(h) *Search programs*.

(1) The licensee must establish and implement searches through the use of technology or personnel to detect, deter, and prevent the introduction of unauthorized firearms, explosives, incendiary devices, or other items which could be used to commit radiological sabotage. The licensee must search individuals, vehicles, and materials consistent with the physical protection program design requirements in paragraph (b) of this section, and the function to be performed at each access control point or portal before granting access into the protected area, and where necessary to meet the performance objectives, in the owner controlled area.

(i) Licensees that meet the requirements of § 73.55(b)(3)(iii) must be capable of detecting and denying unauthorized access to persons and pass-through of contraband materials (e.g., weapons, incendiary devices, explosives) to protected areas.

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

(iii) Searches at vehicle access control points must be monitored to ensure that a response can be initiated if needed.

(2) Prior to granting access to the protected area, licensees must search all personnel, vehicles and materials to meet the requirements of § 73.55(h)(1) and ensure that all items are clearly identified.

(i) The licensee must subject all persons to search upon entry to the protected area except for official Federal, State, and local law enforcement personnel on official duty or individuals under the active protection of the United States Secret Service. Armed response personnel who are on duty and have exited the protected area may re-enter the protected area without being searched for firearms.

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

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

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

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

(i) *Detection and assessment systems*.

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

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

stations, at least one of which must be protected in accordance with the requirements of the central alarm station within this section.

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

(i) Detect both attempted and actual penetration of the protected area perimeter barrier.

(ii) Provide real-time and play-back/recorded video images of the detected activities adjacent to the protected area perimeter barrier before and after each alarm annunciation.

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

(iv) 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.

(v) Ensure intrusion detection and assessment equipment at the protected area perimeter remains operable from an uninterruptible power supply in the event of the loss of normal power.

(4) Alarm stations.

(i) Both alarm stations required by paragraph (i)(2) of this section must be designed and equipped to ensure that a single act, in accordance with the design basis threat of radiological sabotage defined in § 73.1(a)(1), cannot disable both alarm stations. The licensee must ensure the survivability of at least one alarm station to maintain the ability to perform the following functions:

(A) Detect and assess alarms;

(B) Initiate and coordinate an adequate response to an alarm;

(C) Summon offsite assistance; and

(D) Provide command and control.

(ii) Licensees must:

(A) Locate the central alarm station inside a protected area.

(B) Continuously staff each alarm station with at least one trained and qualified alarm station operator. The alarm station operator must not be assigned other duties or responsibilities which would interfere with the ability to execute the functions described in § 73.55(i)(4)(i) of this section.

(C) Ensure that an alarm station operator cannot change the status of a detection point or deactivate a locking or access control device at a protected or vital area portal, without the knowledge and concurrence of the alarm station operator in the other alarm station.

(D) Ensure that operators in both alarm stations are knowledgeable of the final disposition of all alarms.

(5) Surveillance, observation, and monitoring.

(i) The physical protection program must include surveillance, observation, and monitoring as needed to satisfy the design requirements of § 73.55(b), identify indications of tampering, or otherwise implement the site protective strategy.

(ii) [Reserved]

(6) Illumination.

(i) The licensee must ensure that all areas of the facility are provided with illumination, low-light, or other equivalent technology necessary to satisfy the design requirements of § 73.55(b) and implement the protective strategy.

(ii) [Reserved]

(j) *Communication requirements*.

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

(2) A method of communication between alarm stations and security personnel must remain operable from independent power sources in the event of the loss of normal power.

(k) *Response requirements*.

(1) Response performance objective.

(i) The licensee must establish and maintain, at all times, properly trained, qualified and equipped personnel required to interdict and neutralize threats up to and including the design basis threat of radiological sabotage as defined in § 73.1, to prevent a release of radionuclides from any source from exceeding the dose reference values defined in § 50.34(a)(1)(ii)(D)(*1*) and (*2*), § 52.79(a)(1)(vi)(A) and (B), or § 53.210 of this chapter, as applicable.

(ii) [Reserved]

(2) Armed response personnel.

(i) The licensee must provide armed response personnel consisting of armed responders which may be augmented with armed security officers to carry out armed response duties within predetermined timelines specified by the site protective strategy.

(ii) [Reserved]

(3) Armed responders.

(i) The licensee must determine the minimum number of armed responders necessary to satisfy the design requirements of § 73.55(b) and implement the protective strategy. The licensee must document this number in the security plans.

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

(4) Armed security officers.

(i) Armed security officers, designated to strengthen onsite response capabilities, must be onsite and available at all times to carry out their assigned response duties.

(ii) The minimum number of armed security officers designated to strengthen onsite response capabilities must be documented in the security plans.

(5) Alternative response requirements.

(i) The licensee may fulfill the requirements of § 73.55(k)(1) through (4) through alternative means provided that the alternative is described in the physical security plan

and that a technical basis is maintained for demonstrating compliance with the performance requirements of § 73.55(b).

(A) A licensee with prior approval by the Commission may entirely rely on law enforcement or other offsite armed responders.

(B) Structures, systems, and components relied on for delay functions must be designed to allow for timely security responses to adversary attacks with adequate defense in depth.

(ii) [Reserved]

(6) Offsite armed response personnel.

(i) A licensee relying entirely or partially on law enforcement or other off site armed responders must:

(A) Fully describe in the safeguards contingency plan the role that law enforcement or other offsite armed responders will implement in the licensee's protective strategy. The description must provide sufficient detail to enable the NRC to determine that the licensee's physical protection program provides reasonable assurance of adequate protection against threats up to and including the design basis threat of radiological sabotage; and

(B) The physical protection program must be designed to provide layers of security response, with each layer assuring that a single failure does not result in the loss of capability to neutralize the design basis threat adversary.

(C) Provide timely security response to interdict and neutralize adversary attacks up to and including the design basis threat of radiological sabotage.

(D) The security response may rely on the use of onsite responders, law enforcement or other offsite armed responders, or a combination thereof, to fulfill the interdiction and neutralization functions required by paragraph (b)(3)(i) of this section. A licensee relying entirely or partially on law enforcement or other offsite armed responders must—

(*1*) Maintain the capability to detect, assess, interdict, and neutralize threats as required by paragraphs (b)(3)(i) and (b)(3)(ii) of this section;

(*2*) Provide adequate delay to enable law enforcement or other offsite armed responders to fulfill the interdiction and neutralization functions for threats up to and including the design basis threat of radiological sabotage;

(*3*) Identify criteria and measures to compensate for the degradation or absence of law enforcement or other offsite armed responders and propose suitable compensatory measures that meet the requirements of paragraph (o) of this section.

(*4*) For licensees relying entirely or partially on law enforcement responders to fulfill the interdiction and neutralization functions required by paragraph (b)(3)(i) of this section, the training and qualification requirements related to armed response personnel in paragraphs (d) of this section do not apply to law enforcement responders. The licensee must continue to satisfy the performance evaluation requirements in paragraph (b)(5) of this section for all armed response personnel, including law enforcement.

(*5*) Provide necessary information about the facility and make available periodic training to law enforcement or other offsite armed responders who will fulfill the interdiction and neutralization functions for threats up to and including the design basis threat of radiological sabotage.

(ii) [Reserved]

(7) Protective strategy.

(i) The licensee must establish, maintain, and implement a written protective strategy in accordance with the requirements of this section and part 73, appendix C, section II. Upon receipt of an alarm or other indication of a threat, the licensee must implement its safeguards contingency plan.

(ii) [Reserved]

(8) Law enforcement liaison.

(i) To the extent practicable, licensees must document and maintain current agreements with applicable law enforcement agencies to include estimated response times and capabilities.

(ii) [Reserved]

(9) Heightened security.

(i) Licensees must establish, maintain, and implement a threat warning system which identifies specific graduated protective measures and actions to be taken to increase licensee preparedness against a heightened security threat.

(ii) Licensees must ensure that the specific protective measures and actions identified for each threat level are consistent with the security plans and other emergency plans and procedures.

(iii) Upon notification by an authorized representative of the Commission, licensees must implement the specific threat level indicated by the Commission representative.

(l) *Safety/Security Interface*.

(1) The licensee must assess and manage the potential for adverse effects on safety and security, including the site emergency plan, before implementing changes to plant configurations, facility conditions, or security.

(2) [Reserved]

(m) *Security program reviews*.

(1) The licensee must establish and implement security reviews to assess the effectiveness of the implementation of the physical protection program. Security reviews must be 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.

(2) The licensee must review each element of the physical protection program at a frequency commensurate with the importance or significance to safety of plant operations to ensure timely identification and documentation of vulnerabilities,

improvements, and corrective actions. The objective of these reviews must be to maintain effective implementation of the engineered and administrative controls required to achieve the physical protection program functions, and the management system required to implement programs and requirements in this section.

(3) The licensee must establish and perform self-assessments to ensure the effective implementation of the physical protection program functions of detection, assessment, communication, delay, and interdiction and neutralization to protect against the design basis threat of radiological sabotage. As applicable, the licensee must perform design verification and assessments of the capabilities of active and passive engineering systems relied on to protect against the design basis threat.

(4) Reviews of the security program must include, but are not limited to, an audit of the effectiveness of the physical protection program, security plans, implementing procedures, cybersecurity programs, safety/security interface activities, the testing, maintenance, and calibration program, and response commitments by local, State, and Federal law enforcement authorities.

(5) The results and recommendations of the onsite physical protection program reviews, management's findings regarding program effectiveness, and any actions taken as a result of recommendations from prior program reviews, must be documented in a report and must be maintained in an auditable form and available for inspection.

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

(1) The licensee must:

(i) Establish, maintain, and implement a maintenance, testing and calibration program to ensure that security systems and equipment, including secondary and uninterruptible power supplies, are tested for operability and performance at predetermined intervals, maintained in operable condition, and are capable of performing their intended functions.

(ii) Describe the maintenance, testing and calibration program in the physical security plan. Implementing procedures must specify operational and technical details

required to perform maintenance, testing, and calibration activities to include, but not limited to, purpose of activity, actions to be taken, acceptance criteria, and the intervals or frequency at which the activity will be performed.

(iii) The licensee must implement corrective actions to ensure resolution of identified vulnerabilities and deficiencies to satisfy the requirements of this section.

(iv) Security equipment or systems must be tested in accordance with the site maintenance, testing and calibration procedures before being placed back in service after each repair or inoperable state.

(2) [Reserved]

(o) *Compensatory measures*.

(1) The licensee must identify criteria and measures to compensate for degraded or inoperable equipment, systems, and components to meet the requirements of this section.

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

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

(p) *Suspension of security measures*.

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

(i) In accordance with §§ 50.54(x) and 50.54(y) or § 53.740(h) of this chapter, the licensee may suspend any security measures under this section in an emergency when this action is immediately needed to protect the public health and safety and no action consistent with license conditions and technical specifications that can provide adequate or equivalent protection is immediately apparent. This suspension of security measures

must be approved as a minimum by a licensed senior operator or a generally licensed reactor operator before taking this action.

(ii) During severe weather, the licensee may suspend any security measures under this section when this action is immediately needed to protect the personal health and safety of security force personnel and no other immediately apparent action consistent with the license conditions and technical specifications can provide adequate or equivalent protection. This suspension of security measures must be approved, as a minimum, by a licensed senior operator or a generally licensed reactor operator, as applicable, with input from the security supervisor or manager, before taking this action.

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

(3) The suspension of security measures must be reported and documented in accordance with the provisions of §§ 73.1200 and 73.1205 of this part.

(q) *Records*.

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

(2) The licensee must maintain all records required to be kept by Commission regulations, orders, or license conditions, until the Commission terminates the license for which the records were developed, and must maintain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the Commission.

(3) The licensee must retain, in accordance with § 73.70, all analyses, assessments, calculations, and descriptions of the technical basis for demonstrating compliance with the performance requirements of this section. The licensee must protect these records in accordance with the requirements for protecting safeguards information in §§ 73.21 and 73.22.

(4) If a contracted security force is used to implement the onsite physical protection program, the licensee's written agreement with the contractor must be retained by the licensee as a record for the duration of the contract.

(5) Review and audit reports must be maintained and available for inspection, for a period of 3 years.

(r) *Alternative measures*.

(1) The Commission may authorize an applicant or licensee to provide a measure for protection against radiological sabotage other than one required by this section if the applicant or licensee demonstrates that:

(i) The measure meets the same performance objectives and requirements specified in paragraph (b) of this section; and

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

(2) The licensee must submit proposed alternative measure(s) to the Commission for review and approval in accordance with § 50.4 and § 50.90, or § 53.040 and § 53.1510 of this chapter before implementation.

(3) In addition to fully describing the desired changes, the licensee must submit a technical basis for each proposed alternative measure. The basis must include an analysis or assessment that demonstrates how the proposed alternative measure provides a level of protection that is at least equal to that which would otherwise be provided by the specific requirement of this section.

(4) The licensee may implement alternatives from the following specific requirements through the use of technology, without prior Commission approval, provided that the alternative is described in the physical security plan and that a technical basis is maintained for demonstrating compliance with the performance requirements of § 73.55(b):

(i) The requirement in paragraph (d)(2) of this section that a member of the security organization who has the authority to direct the activities of the security organization be onsite at all times;

(ii) The requirement in paragraph (e)(3) of this section that the reactor control room, the central alarm station, and the location within which the last access control function for access to the protected area is performed be bullet-resisting.

66. Amend § 73.56 as follows:

a. Revise the section heading;

b. Revise paragraph (a)(1);

c. Remove and reserve paragraphs (a)(2) and (3);

d. Revise paragraphs (c) and (d)(3);

e. In paragraph (f)(3), remove the phase “re-evaluation or ”;

f. In the heading for paragraph (h)(4)(ii)(A), remove the word “Update” and add in its place the word “Reinstatements”;

g. Revise paragraph (h)(4)(ii)(B);

h. Revise paragraphs (i)(1)(iv) and (i)(1)(v)(A), the introductory text to paragraphs (i)(1)(v)(B) and (i)(1)(v)(B)(*4*), and paragraph (j);

i. In paragraph (n)(1), remove the number “24” wherever it may appear and add in its place the number “36”; and in paragraph (n)(2), remove the number “12” wherever it may appear and add in its place the number “24”;

j. In paragraph (n)(6), remove the reference “§ 73.55(b)(10)” and add in its place the reference “§ 73.55(b)(9)”; and

k. In paragraphs (o)(2), remove the number “5” wherever it may appear and add in its place the number “3”.

The revisions and additions to read as follows:

§ 73.56 Personnel access authorization requirements for commercial nuclear power plants.

(a) * * *

(1) Except as described in § 73.120(a), each applicant for an operating license under the provisions of part 50 of this chapter, each holder of a combined license under the provisions of part 52 of this chapter, and each applicant for an operating license or holder of a combined license under part 53 of this chapter must implement the requirements of this section before initial fuel load into the reactor (or, for a fueled manufactured reactor, before initiating the removal of features to prevent criticality).

* * * * *

(c) *General performance objective.* The licensee's or applicant's access authorization program must provide reasonable assurance that the individuals who are specified in paragraph (b)(1), and, if applicable, paragraph (b)(2) of this section are trustworthy and reliable, such that they do not constitute an unreasonable risk to public health and safety or the common defense and security, including the potential to commit radiological sabotage.

(d) * * *

(3) *Verification of true identity.* Licensees, applicants, and contractors or vendors shall verify the true identity of an individual who is applying for unescorted access or unescorted access authorization in order to ensure that the applicant is the person that he or she has claimed to be. As part of this verification, licensees and applicants shall determine whether the results of the fingerprinting required under § 73.57 confirm the individual's claimed identity, if such results are available.

* * * * *

(h) * * *

(4) * * *

(ii) * * *

(B) *Update of unescorted access or unescorted access authorization.* For individuals whose last unescorted access or unescorted access authorization status has been interrupted for greater than 365 calendar days but fewer than 3 years the licensee,

applicant or contractor or vendor shall evaluate the period of time since the individual last held unescorted access or unescorted access authorization status, up to and including the day the individual applies for updated unescorted access authorization. For the 1-year period preceding the date upon which the individual applies for unescorted access authorization, the licensee, applicant, or contractor or vendor shall ensure that the employment history evaluation is conducted with every employer, regardless of the length of employment. For the remaining period, the licensee, applicant or contractor or vendor shall ensure that the employment history evaluation is conducted with the employer by whom the individual claims to have been employed the longest within each calendar month. In addition, the individual shall be subject to the psychological assessment required in § 73.56(e).

* * * * *

(i) * * *

(1) * * *

(iv) The individual's supervisor interacts with the individual with a frequency that allows the supervisor to form an informed and reasonable opinion regarding the individual's behavior, trustworthiness, and reliability; or the individual is subject to an annual (within 365 calendar days) supervisory review conducted in accordance with the requirements of the licensee's or applicant's behavioral observation program.

(v) * * *

(A) A criminal history update for any individual with unescorted access. The criminal history update must be completed within 5 years of the date on which these elements were last completed or, for licensees or approved applicants that participate in a U.S. Government monitoring and notification program through a Memorandum of Understanding with the NRC, within 10 years of the date on which these elements were last completed.

(B) For individuals who perform one or more of the job functions described in this paragraph that are critical to the safe and secure operation of the facility, the

trustworthiness and reliability determination must be based on a criminal history update within 5 years of the date on which these elements were last completed or, for licensees or approved applicants that participate in a U.S. Government monitoring and notification program through a Memorandum of Understanding with the NRC, within 10 years of the date on which these elements were last completed, or more frequently, based on job assignment as determined by the licensee or applicant; and a psychological re-assessment within 5 years of the date on which this element was last completed:

* * * * *

(*4*) Individuals who have access, extensive knowledge, or administrative control over plant digital computer and communication systems and networks as identified in § 73.54 or § 73.110, as applicable, including—

* * * * *

(j) *Access to vital areas.* Licensees or applicants shall establish, implement, and maintain a list of individuals who are authorized to have unescorted access to specific nuclear power plant vital areas during non-emergency conditions. The list must include only those individuals who have a continued need for access to those specific vital areas in order to perform their duties and responsibilities. The list must be approved by a cognizant licensee or applicant manager or supervisor who is responsible for directing the work activities of the individual who is granted unescorted access to each vital area, and updated and re-approved no less frequently than every 31 days or, for licensees that participate in a U.S. Government monitoring and notification program through a Memorandum of Understanding with the NRC, no less frequently than every 6 months.

* * * * *

67. In § 73.57, revise paragraph (b)(2)(v) to read as follows:

§ 73.57 Requirements for criminal history records checks of individuals granted unescorted access to a nuclear power facility, a non-power reactor, or access to Safeguards Information.

* * * * *

(b) * * *

(2) * * *

(v) Individuals who have a valid unescorted access authorization to a non-power reactor facility on November 7, 2012, are not required to undergo a new fingerprint-based criminal history records check pursuant to paragraph (g) of this section, until such time that the existing authorization expires, is terminated, or is otherwise to be renewed.

* * * * *

§ 73.58 [Reserved]

68. Remove and reserve § 73.58.

69. In § 73.59, revise paragraph (j) to read as follows:

§ 73.59 Relief from fingerprinting, identification and criminal history records checks and other elements of background checks for designated categories of individuals.

* * * * *

(j) Representatives of the International Atomic Energy Agency (IAEA) who have been certified by the NRC;

* * * * *

§ 73.61 [Amended]

70. In § 73.61(h), remove the phase “engaged in activities associated with the U.S./IAEA Safeguards Agreement”.

71. In § 73.67, revise paragraphs (b)(1)(i), (d), and the introductory text of paragraph (f) to read as follows:

§ 73.67 Licensee fixed site and in-transit requirements for the physical protection of special nuclear material of moderate and low strategic significance.

* * * * *

(b) * * *

(1) * * *

(i) Special nuclear material which is not readily separable from other radioactive material and which has a total external radiation level more than 1 gray (100 rad) per hour at 1 meter (3.3 feet) from any accessible surface without intervening shielding, or

* * * * *

(d) *Fixed site requirements for special nuclear material of moderate strategic significance.* Except as allowed by paragraph (b)(2) of this section and except those who are licensed to operate a nuclear power reactor pursuant to part 50, part 52, or part 53 of this chapter, provided that the special nuclear material is located within a protected area and protected under § 73.55 or § 73.100, each licensee who possesses, stores, or uses quantities and types of special nuclear material of moderate strategic significance at a fixed site or contiguous sites must meet the following general performance objectives and requirements, in addition to those in paragraph (a) of this section:

(1)(i) Store or use the material only within a controlled access area;

(ii) Provide prompt detection and assessment of unauthorized access or activities by an external adversary within the controlled access area,

(iii) Provide prompt detection of removal of special nuclear material by an external adversary from a controlled access area.

(iv) Mitigate the risk of bulk theft of special nuclear material;

(v) Delay an external adversary from completing a bulk theft of special nuclear material sufficiently to allow response forces to impede the adversary and facilitate recovering the special nuclear material;

(vi) Analyze and identify in the security plan site-specific conditions that may affect the specific measures needed to implement the requirements of this subpart and must account for these conditions in the design of the physical protection program;

(vii) Provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and security implementing procedures as needed to ensure the effectiveness of the physical protection program;

(viii) Coordinate the implementation of the security plan and associated procedures with other onsite plans and procedures to preclude conflict during normal conditions and minimize conflict during emergency conditions;

(ix) Assess and manage the potential for adverse effects on safety, security, and material control and accounting before implementing changes to facility configurations, facility conditions, or security;

(x) Communicate potential conflicts among safety, security, and material control and accounting to appropriate licensee personnel and take compensatory and/or mitigating actions to maintain safety, security, and material control and accounting at the facility.

(2) In addition, the licensee must:

(i) Establish and maintain written response procedures for dealing with threats of thefts or thefts of Category II quantities of SNM.

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

(iii) Identify and analyze site-specific conditions to determine the specific use, type, function, and placement of physical barriers needed to delay an external adversary from removal of special nuclear material and completing a vehicle-assisted bulk theft of special nuclear material to allow response forces to impede the adversary or facilitate recovery of the special nuclear material.

(iv) Establish an access authorization program to include a background investigation to ensure that the individuals granted unescorted access to special nuclear material are trustworthy and reliable. The background investigation must include at a minimum:

(A) Consideration of criminal history based on fingerprinting and an FBI identification and criminal history records check in accordance with § 73.57;

(B) Verification of the true identity of the individual who is applying for unescorted access to ensure that the applicant is who he or she claims to be;

(C) Verification of employment history, including military history;

(D) Verification of the individual's educational history; and

(E) Consideration of an individual's character and reputation determination.

(v) Monitor with an intrusion alarm or other device or procedures the controlled access areas to detect unauthorized penetration or activities involving Category II quantities of SNM.

(vi) Provide surveillance, observation, and monitoring, as needed, to satisfy the general performance objective and requirements, and identify indications of tampering of components of the physical protection program including, but not limited to, barriers, access control devices, and intrusion detection equipment.

(vii) Establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations.

(viii) To the extent practicable, document and maintain current agreements with applicable law enforcement agencies to include estimated response times and capabilities. In addition, the licensee must provide necessary information about the site and nuclear material locations and make available periodic training to law enforcement to support response actions.

(ix) Establish, implement, and maintain a threat warning system that identifies specific graduated protective measures and actions to be taken to increase licensee preparedness against a heightened security threat.

(x) Upon receipt of an alarm or other indication of a threat, determine the existence and level of the threat in accordance with pre-established assessment methodologies, initiate response actions to promptly detect attempts to remove SNM and notify local law enforcement agencies to recover SNM in accordance with security implementing procedures.

(xi) Review each element of the physical protection program:

(A) At least every 24 months;

(B) More frequently as necessary based upon site-specific analysis, assessments, or other performance indicators; and

(C) Within 12 months following initial implementation of the physical protection program or a change in personnel, procedures, equipment, or facilities that could adversely affect security.

(xii) Establish, maintain, and implement a maintenance, testing, and calibration program to ensure that physical protection systems and equipment, including secondary and uninterruptible power supplies, are tested for operability and performance at predetermined intervals, maintained in operable condition, and can perform their intended functions.

(xiii) Identify criteria and measures to compensate for degraded or inoperable equipment, systems, and components of the physical protection program.

(A) Compensatory measures must provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable equipment, systems, or components, when fully functional.

(B) Compensatory measures must be implemented within specific timeframes necessary to meet the general performance objective and requirements and described in the security plan.

(C) Compensatory measures must not be used in lieu of performing timely repair on the degraded or inoperable equipment, systems, or components.

(xiv) Maintain all reports, records, or documents required to be kept by Commission regulations, orders, or license conditions, until the Commission terminates the license for which the records were developed and must maintain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the Commission.

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

(B) If a contracted security force is used to implement the onsite physical protection program, the licensee's written agreement with the contractor must be retained by the licensee as a record for the duration of the contract.

(C) Review and audit reports must be maintained and available for inspection, for a period of 3 years.

(3) In addition to the fixed-site requirements set forth in this section, the Commission may incorporate or eliminate, depending on the individual facility and site conditions, any existing, alternate, or additional measures deemed necessary to protect against theft or diversion of Category II special nuclear material.

(4) *Alternative measures.* The Commission may authorize an applicant or licensee to use a measure other than one required by this section, if the applicant or licensee demonstrates that the measure meets the same performance objectives and requirements in paragraphs (a) and (b)(1) of this section.

(i) The licensee must submit the proposed alternative measures to the Commission for review and approval in accordance with § 50.90, § 53.1510, or § 70.34 of this chapter, as applicable, before implementation.

(ii) In addition to fully describing the desired changes, the licensee must submit a technical basis for each proposed alternative measure. The basis must include an analysis or assessment that demonstrates how the proposed alternative measure provides a level of protection that is at least equal to that which would otherwise be provided by the specific requirement of this subpart for which the alternative measure is proposed.

* * * * *

(f) *Fixed site requirements for special nuclear material of low strategic significance.* Each licensee who possesses, stores, or uses special nuclear material of low strategic significance at a fixed site or contiguous sites, except those who are licensed to operate a nuclear power reactor pursuant to part 50, part 52, or part 53, provided that the special nuclear material is located within a protected area and protected under § 73.55 or § 73.100, shall:

* * * * *

§ 73.70 [Amended]

72. In § 73.70, in paragraph (b), remove the phrase “and badge numbers” and add in its place the phrase “badge numbers or a personnel identification system”; and in paragraph (d), remove the phrase “badge number” and add in its place the phrase “badge number or personnel identification system”.

73. Revise § 73.77 to read as follows:

§ 73.77 Cybersecurity event notifications.

(a) Each licensee subject to the provisions of § 73.54 or § 73.110 must notify the NRC Headquarters Operations Center of a cyberattack that adversely impacted a safety or security function using the procedures of § 50.72 or § 53.1630 of this chapter or § 73.1200 of this part based on the function adversely impacted (safety or security).

(b) If it is later determined that the cause of a previously reported event was from a cyberattack, the NRC shall be notified using one of the following applicable methods:

(1) Follow up notification process as specified in § 50.72 or § 53.1630 of this chapter;

(2) Significant supplemental information process as specified in § 73.1200 of this part; or

(3) Submission of a Licensee Event Report as specified in § 50.73 or § 53.1640 of this chapter, or § 73.1205 of this part.

74. In § 73.100, revise paragraph (a)(1) to read as follows:

Subpart J—Security Notifications, Reports, and Recordkeeping

§ 73.100 Technology-inclusive requirements for physical protection of licensed activities at commercial nuclear plants against radiological sabotage.

(a) * * *

(1) Each licensee that is licensed to operate a commercial nuclear plant under 10 CFR part 53 of this chapter and elects to implement the requirements of this section, and each licensee that is licensed to operate a nuclear power plant under 10 CFR part 50 or 52 of this chapter after [EFFECTIVE DATE] and elects to implement the requirements of this section, must identify achievable target sets in accordance with paragraph (b)(5) of this section and develop, implement, and maintain a physical protection program under the following requirements:

* * * * *

75. In § 73.110, revise paragraph (a) and the introductory text to paragraph (b) to read as follows:

§ 73.110 Technology-inclusive requirements for protection of digital computer and communication systems and networks.

(a) Each licensee that is licensed to operate a commercial nuclear plant under 10 CFR part 53 and elects to implement the requirements of this section, and each licensee that is licensed to operate a nuclear power plant under 10 CFR part 50 or 52 after [EFFECTIVE DATE] and elects to implement the requirements of this section, must establish, implement, and maintain a cybersecurity program that is commensurate with the potential consequences resulting from cyberattacks, up to and including the design basis threat as described in § 73.1 of this part. The cybersecurity program must provide reasonable assurance that digital computer and communication systems and networks are adequately protected against cyberattacks that are capable of causing the following consequences:

(1) Adversely impacting the safety, security, and emergency preparedness functions performed by digital assets that prevent a postulated fission product release resulting in offsite doses exceeding the values in § 50.34(a)(1)(ii)(D), § 52.47(a)(2)(iv), or § 53.210 of this chapter, as applicable.

(2) Adversely impacting the security functions performed by digital assets necessary for implementing the physical security requirements in § 53.860(a) of this chapter or § 73.55 of this part, as applicable.

(b) To protect digital computer and communication systems and networks associated with the functions described in paragraphs (a)(1) and (2) of this section (including support systems and equipment which if compromised adversely impact these functions), the licensee must—* * *

* * * * * *

76. In § 73.120, revise paragraph (a) to read as follows:

§ 73.120 Access authorization program for commercial nuclear plants.

(a) *Introduction and scope*.

(1) Each applicant for or holder of an operating license or combined license under part 50, 52, or 53 of this chapter, who demonstrates compliance with §

73.55(a)(1)(i) or § 73.100(a)(1)(i), as applicable, must establish, maintain, and implement an access authorization program that meets the requirements of this section before initial fuel load into the reactor (or, for a fueled manufactured reactor, before initiating the removal of features to prevent criticality).

(2) The licensee or applicant may accept, in part or whole, an access authorization program implemented by a contractor or vendor to satisfy appropriate elements of their access authorization program in accordance with the requirements of this section. Only a licensee may grant an individual unescorted access, and only a licensee or applicant may certify an individual's unescorted access authorization. Licensees and applicants are responsible for maintaining, denying, terminating, or withdrawing unescorted access authorization.

* * * * *

77. Amend § 73.1200 as follows:

a. Revise the section heading;

b. Revise paragraph (b)(3)(ii);

c. Revise and republish paragraph (c)(1)(i);

d. Revise paragraphs (e)(1)(iv) and (v), (e)(2), and (e)(3)(i), (g)(1), the introductory text to paragraphs (m)(1) and (n)(1), and paragraph (o)(3);

e. Redesignate paragraph (q)(2) as paragraph (q)(3) and add new paragraph (q)(2); and

f. Revise paragraphs (s) and (t).

The revisions and additions to read as follows:

§ 73.1200 Notification of security events.

* * * * *

(b) * * *

(3) * * *

(ii) Briefly describe the nature of the hostile action or event, including:

(A) Type of hostile action or event (e.g., armed assault, vehicle bomb, theft of shipment, sabotage, etc.); and

(B) The current status (i.e., imminent, in progress, or neutralized).

* * * * *

(c) * * *

(1) * * *

(i) 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:

(A) The theft or diversion of a Category I, II, or III quantity of SSNM; a Category II or III quantity of special nuclear material (SNM); SNF; or HLW;

(B) Significant physical damage to any nuclear power reactor, to a facility possessing a Category I or II quantity of SSNM, or to a facility storing or disposing of SNF and/or HLW;

(C) The unauthorized operation, manipulation, or tampering with any nuclear power reactor's controls or with structures, systems, and components (SSCs) that results in the interruption of normal operation of the reactor; or

(D) The unauthorized operation, manipulation, or tampering with any Category I SSNM facility's SSCs that results in an accidental criticality.

* * * * *

(e) * * *

(1) * * *

(iv) The attempted introduction of contraband into a PA, VA, or MAA;

(v) The discovery that a weapon that is authorized by the licensee's security plan is lost within a PA, VA, or MAA;

* * * * *

(2) An event related to the licensee's implementation of their security program for which a notification was made to local, State, or Federal law enforcement officials (other than a suspicious activity report made under § 73.1215 of this part) provided that the

event does not otherwise require a notification under paragraphs (a) through (h) of this section.

(3)(i) An event involving a law enforcement response to the facility that could reasonably be expected to result in public or media inquiries and that does not otherwise require a notification under paragraphs (a) through (h) of this section, or in other NRC regulations such as § 50.72(b), § 53.1630(b), or § 72.75(b)(2) of this chapter, or under § 73.1215 of this part.

* * * * *

(g) *Eight-hour notifications—facilities.* (1) Each licensee subject to the provisions of § 73.20, § 73.45, § 73.46, § 73.50, § 73.51, § 73.55, § 73.60, § 73.67, or § 73.100 must notify the NRC Headquarters Operations Center within 8 hours after time of discovery of the following facility security program failures or cybersecurity events involving—

(i) Any failure, degradation, or vulnerability in a security or safeguards system, for which compensatory measures have not been employed within the required timeframe, that could allow unauthorized or undetected access of—

(A) Unauthorized personnel into a PA, VA, MAA, or CAA; or

(B) Contraband into a PA, VA, or MAA;

(ii) The unauthorized operation, manipulation, or tampering with any nuclear power reactor’s controls or with SSCs that does not result in the interruption of normal operation of the reactor;

(iii) The unauthorized operation, manipulation, or tampering with any Category I SSNM facility’s SSCs that does not result in the interruption of normal operation of the facility or an accidental criticality; or

(iv) For licensees subject to the provisions of § 73.77 of this part, a cybersecurity event that impacted the ability of the facility’s SSCs to perform their intended security functions.

* * * * *

(m) *Enhanced weapons notifications—stolen or lost.* (1) Each licensee possessing enhanced weapons in accordance with § 73.15 of this part must—

* * * * *

(n) *Enhanced weapons—adverse ATF findings.* (1) Each licensee possessing enhanced weapons in accordance with § 73.15 of this part must—

* * * * *

(o) * * *

(3) Notifications required by this section that *contain* Safeguards Information may be made to the NRC Headquarters Operations Center without using secure communications systems under the exception of § 73.22(f)(3) of this part for the communication of emergency or extraordinary conditions.

* * * * *

(q) * * *

(2) Licensees desiring to retract a previous cybersecurity event notification made under paragraph (g) of this section, which has been determined to be invalid or not reportable in accordance with the requirements of paragraph (g) of this section must telephonically notify the NRC Headquarters Operations Center in accordance with paragraph (o) of this section and indicate the report that is being retracted and the basis for the retraction.

* * * * *

(s) *Elimination of duplication.*

(1) Licensees with notification obligations under paragraphs (a) through (h), (m), and (n) of this section and § 50.72, 53.1630, 63.73, 70.50, 72.75, or 95.57 of this chapter may notify the NRC of events in a single communication.

(2) A licensee notifying the NRC of multiple events in a single communication must identify each regulation under which the licensee is reporting an event.

(t) *Classified information.*

(1) A licensee's notifications regarding security events associated with the deliberate disclosure, theft, loss, compromise, or possible compromise of classified documents, information, or material must comply with the requirements found in § 95.57 of this chapter.

(2) A licensee notifying the NRC of an event involving both information security issues (regarding classified documents, information, or material) pursuant to § 95.57 of this chapter and physical security issues pursuant to paragraphs (a) through (h), (m), and (n) of this section, may notify the NRC in a single communication under paragraph (s) of this section.

78. In § 73.1205, revise the section heading and paragraphs (a)(2) and (e) to read as follows:

§ 73.1205 Written follow-up reports of security events.

(a) * * *

(2) As an exemption, licensees are not required to submit a written follow-up report subsequent to a telephonic notification made—

(i) Under the provisions of §§ 73.1200(a) and (b) regarding 15-minute event notifications;

(ii) Under the provisions of §§ 73.1200(g) and (h) regarding 8-hour event notifications;

(iii) Under the provisions of §§ 73.1200(e) and (f) regarding interactions with a Federal, State, or local law-enforcement agency;

(iv) Under the provisions of § 73.1200(m) regarding lost or stolen enhanced weapons; or

(v) Under the provisions of § 73.1200(n) regarding adverse findings from the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) for enhanced weapons possessed by the licensee.

* * * * *

(e) *Records retention.* Licensees must maintain a copy of a written follow-up report as a record for a period of 3 years from the date of the report or until termination of the license, whichever is earlier.

79. In § 73.1210, revise the section heading, paragraphs (b)(2) and (3)(iii), and paragraph (e) to read as follows:

§ 73.1210 Recordkeeping of security events.

* * * * *

(b) * * *

(2) Licensees must retain these records for a period up to 3 years after the last entry is recorded, or until their license is terminated, whichever is earlier.

(3) * * *

* * * * *

(iii) Licensees must ensure that Safeguards Information or classified security information associated with these records is created, stored, and handled in accordance with the provisions of §§ 73.21 and 73.22 of this part, or of part 95 of this chapter, as applicable.

* * * * *

(e) *Uncontrolled weapons events*.

(1) The discovery that an authorized weapon is uncontrolled within a licensee's PA, VA, or MAA.

(2) Uncontrolled authorized weapons are defined as weapons that are authorized under the licensee's security plan and are not in the possession of authorized personnel or are not in an authorized weapons' storage location.

* * * * *

80. In § 73.1215:

a. Revise paragraphs (a) and (c);

b. In paragraph (d)(1)(v), remove the phrase “aircraft activities” and add in its place the phrase “crewed/uncrewed aviation-related assets engaging in overflight activities”.

The revisions read as follows:

§ 73.1215 Suspicious activity reports.

(a) *Purpose.* This section sets forth the reporting criteria and process for licensees to use in reporting suspicious activities. Licensees are required to report suspicious activities to the local law enforcement agency (LLEA), the applicable Federal Bureau of Investigation (FBI) field office, the NRC, and the applicable Federal Aviation Administration (FAA) facility if crewed/uncrewed aviation-related assets are a part of the suspicious activity.

* * * * *

(c) *General requirements.*

(1)(i) Licensees subject to paragraphs (d), (e), and (f) of this section must report suspicious activities that are applicable to their facility, material, or shipping activity.

(ii) If a suspicious activity requires a physical security event notification pursuant to § 73.1200, then the licensee is not required to also report the occurrence as a suspicious activity pursuant to this section.

(iii) If a suspicious activity report results in a LLEA response the licensee must notify the NRC in accordance with the requirements of § 73.1200.

(iv) Licensees subject to paragraph (d) of this section and part 37 of the chapter who are reporting suspicious activities at their facility per this section are not required to submit a duplicate report under § 37.57 of this chapter.

(2)(i) Licensees must promptly assess whether an activity is suspicious. Licensees may review additional information as part of an assessment process, including interactions with their LLEA. However, such assessments and any subsequent reporting must be completed as soon as possible, but within 4 hours of the time of

discovery. The licensee must base its assessment upon its best available information on the activity, which may include its knowledge of its locale and the local population.

(ii) The licensee's assessment of a potential suspicious activity, and any discussion of this activity with its LLEA, does not constitute a conclusion, in and of itself, that the activity is suspicious.

(iii) Licensees are not required to report activities that, based on their assessment, appear to be innocent or innocuous.

(3) For a suspicious activity specified under paragraph (d) of this section, the licensee must make the following reports. A licensee may depart from the standard order of precedence of these reports, if it determines the circumstances warrant such action:

(i) First, to their LLEA;

(ii) Second, to their applicable FBI field office;

(iii) Third, to the NRC Headquarters Operations Center; and

(iv) Lastly, to the applicable FAA facility if the suspicious activity involves crewed/uncrewed aviation-related assets that are engaged in overflights in proximity to the licensee's facility.

(4) For a suspicious activity specified under paragraphs (e) and (f) of this section, the licensee or its designated movement control center must make the following reports, in the order indicated. A licensee or its movement control center may depart from the standard order of precedence of these reports, if it determines the circumstances warrant such action:

(i) First, to the applicable LLEA;

(ii) Second, to the applicable FBI field office; and

(iii) Lastly, to the NRC Headquarters Operations Center.

(iv) For licensees making such reports related to shipping activities, the licensee responsible for the security of the shipment must contact the applicable FBI field office.

(v) For a movement control center making such reports related to shipping activities, the applicable FBI field office is as requested by the FBI. As such, the FBI may

direct the use of the FBI field office applicable to the movement control center itself or to the FBI field office applicable to the licensee responsible for the security of the shipment.

(5)(i) Licensees subject to paragraphs (d) and (f) of this section must establish a point of contact with their applicable FBI field office.

(ii) Licensees subject to paragraph (d) of this section must establish a point of contact with their applicable FAA facility.

(6)(i) For licensees subject to paragraph (e) of this section who are responsible for the security of the shipment(s), the licensee must establish a point of contact with their applicable FBI field office.

(ii) For licensees subject to paragraph (e) of this section who are employing the services of a movement control center, the movement control center must establish a point of contact with its applicable FBI field office.

(7) Licensees and movement control centers reporting suspicious activities to the NRC must notify the NRC Headquarters Operations Center by the telephone number specified in Table 1 of appendix A of this part.

(8)(i) Licensees and movement control centers reporting suspicious activities must document the LLEA and FBI points of contact in written security communication procedures or route approvals, as applicable.

(ii) Licensees reporting suspicious crewed/uncrewed aviation-related assets engaging in overflight activities must document the FAA point of contact in written communication procedures.

* * * * *

81. In appendix A to part 73, revise and republish table 1 and table 2 to read as follows:

APPENDIX A TO PART 73—U.S. NUCLEAR REGULATORY COMMISSION OFFICES AND CLASSIFIED MAILING ADDRESSES

Table 1—Mailing Addresses, Telephone Numbers, and Email Addresses

	Address	Telephone (24-hour)	Email
NRC Headquarters Operations Center	USNRC, Division of Preparedness and Response, Washington, DC 20555-0001	(301) 816-5100; (301) 816-5151 (fax)	*Hoo.Hoc@nrc.gov; Hoo1@nrc.sgov.gov* (secure).
Region I: Connecticut, Delaware, District of Columbia, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, Rhode Island, and Vermont	USNRC, Region I, 475 Allendale Road, Suite 102, King of Prussia, PA 19406-1415	(610) 337-5000, (800) 432-1156 TDD: (301) 415-5575	*RidsRgn1MailCenter@nrc.gov.*
Region II: Alabama, Florida, Georgia, Kentucky, North Carolina, Puerto Rico, South Carolina, Tennessee, Virginia, Virgin Islands, and West Virginia	USNRC, Region II, 245 Peachtree Center Avenue, NE., Suite 1200, Atlanta, GA 30303-1257	(404) 997-4000, (800) 877-8510, TDD: (301) 415-5575	*RidsRgn2Mail Center@nrc.gov*
Region III: Illinois, Indiana, Iowa, Michigan, Minnesota, Missouri, Ohio and Wisconsin	USNRC, Region III, 2056 Westings Ave, Suite 400, Naperville, IL 60563-2657	(630) 829-9500, (800) 522-3025, TDD: (301) 415-5575	*RidsRgn3MailCenter@nrc.gov*
Region IV: Alaska, Arizona, Arkansas, California, Colorado, Hawaii, Idaho, Kansas, Louisiana, Mississippi, Montana, Nebraska, Nevada, New Mexico, North Dakota, Oklahoma, Oregon, South Dakota, Texas, Utah, Washington, Wyoming, and the U.S. territories and possessions in the Pacific	US NRC, Region IV, 1600 E Lamar Blvd., Arlington, TX 76011-4511	(817) 200-1100, (800) 952-9677, TDD: (301) 415-5575	*RidsRgn4MailCenter@nrc.gov.*

Table 2—Classified Mailing Addresses

	Address
NRC Headquarters	U.S. NRC, 11555 Rockville Pike, P.O. Box 2500, Rockville, MD 20852-2738.
Region I	U.S. NRC, 475 Allendale Road, Suite 102, King of Prussia, PA 19406-1415.
Region II	USNRC, P.O. Box 56267, Atlanta, GA 30343.
Region III	USNRC, Region III, 2056 Westings Ave, Suite 400, Naperville, IL 60563-2657.

Region IV	US NRC, Region IV, 1600 E. Lamar Blvd., Arlington, TX 76011-4511.

* * * * *

82. Revise and republish Appendix B to part 73 to read as follows:

APPENDIX B TO PART 73—GENERAL CRITERIA FOR SECURITY PERSONNEL

Table of Contents

C. Duty Training

D. Duty Qualification and Requalification

E. Weapons Training

F. Weapons Qualification and Requalification Program

G. Weapons Maintenance

H. Records

I. Reviews

J. Definitions

Introduction

Applicants and power reactor licensees subject to the requirements of § 73.55 shall comply with the requirements of section I, “Employment Suitability and Qualification,” paragraphs I.A, I.B.1.a., I.B.1.b.(1),(a) - (b), I.B.1.b.(2),(a) – (c) and section VI of this appendix for armed and unarmed individuals who are assigned security duties. All other licensees, applicants, or certificate holders shall comply only with sections I through V of this appendix.

Security personnel who are responsible for the protection of special nuclear material on site or in transit and for the protection of the facility or shipment vehicle against radiological sabotage should, like other elements of the physical security system, be required to meet minimum criteria to ensure that they will effectively perform their assigned security-related job duties. In order to ensure that those individuals responsible for security are properly equipped and qualified to execute the job duties prescribed for them, the NRC has developed general criteria that specify security personnel qualification requirements.

These general criteria establish requirements for the selection, training, equipping, testing, and qualification of individuals who will be responsible for protecting special nuclear materials, nuclear facilities, and nuclear shipments.

When required to have security personnel that have been trained, equipped, and qualified to perform assigned security job duties in accordance with the criteria in this

appendix, the licensee must establish, maintain, and follow a plan that shows how the criteria will be met. The plan must be submitted to the NRC for approval and must be implemented within 30 days after approval by the NRC unless otherwise specified by the NRC in writing.

Definitions

Terms defined in parts 50, 53, 70, and 73 of this chapter have the same meaning when used in this appendix.

Criteria

I. Employment Suitability and Qualification.

A. Suitability.

1. Before employment, or assignment to the security organization, an individual shall:

a. 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;

b. Have attained the age of 18 for an unarmed capacity; or have attained the age of 18 or the minimum age required by applicable State law for an armed capacity, whichever is older;

c. Not have any felony convictions that reflect on the individual's reliability; and

d. Not be disqualified, in accordance with applicable state or Federal law from possessing or using firearms or ammunition.

(1) Licensees may use the information that has been obtained during the completion of the individual's background investigation for unescorted access to determine suitability; or

(2) Licensees may use the satisfactory completion of a firearms background check for the individual under § 73.17 of this part to also fulfill this requirement.

2. The qualification of each individual to perform assigned duties and responsibilities must be documented.

B. Physical and mental qualifications.

1. Physical qualifications:

a. Individuals whose security tasks and job duties are directly associated with the effective implementation of the licensee physical security and contingency plans shall have no physical weaknesses or abnormalities that would adversely affect their performance of assigned security job duties.

b. In addition to a. above, guards, armed response personnel, armed escorts, and central alarm station operators shall successfully pass a physical examination administered by a licensed physician. The examination shall be designed to measure the individual's physical ability to perform assigned security job duties as identified in the licensee physical security and contingency plans. Armed personnel shall meet the following additional physical requirements:

(1) Vision:

(a) For each individual, distant visual acuity in each eye shall be correctable to 20/30 (Snellen or equivalent) in the better eye and 20/40 in the other eye with eyeglasses or contact lenses. If uncorrected distance vision is not at least 20/40 in the better eye, the individual shall carry an extra pair of corrective lenses. Near visual acuity, corrected or uncorrected, shall be at least 20/40 in the better eye. Field of vision must be at least 70° horizontal meridian in each eye. The ability to distinguish red, green, and yellow colors is required. Loss of vision in one eye is disqualifying. Glaucoma shall be disqualifying, unless controlled by acceptable medical or surgical means, provided such medications as may be used for controlling glaucoma do not cause undesirable side effects which adversely affect the individual's ability to perform assigned security job duties, and provided the visual acuity and field of vision requirements stated above are met. On-the-job evaluation shall be used for individuals who exhibit a mild color vision defect.

(b) The use of corrective eyeglasses or contact lenses shall not interfere with an individual's ability to effectively perform assigned security job duties during normal or emergency operations.

(2) Hearing:

(a) Individuals shall have no hearing loss in the better ear greater than 30 decibels average at 500 Hz, 1,000 Hz, and 2,000 Hz with no level greater that 40 decibels at any one frequency (by ISO 389 "Standard Reference Zero for the Calibration of Puritone Audiometer" (1975) or ANSI S3.6-1969 (R. 1973) "Specifications for Audiometers"). ISO 389 and ANSI S3.6-1969 have been approved for incorporation by reference by the Director of the Federal Register. A copy of each standard is available for inspection at the NRC Library, 11545 Rockville Pike, Rockville, Maryland 20852-2738.

(b) A hearing aid is acceptable provided suitable testing procedures demonstrate auditory acuity equivalent to the above stated requirement.

(c) The use of a hearing aid shall not decrease the effective performance of the individual's assigned security job duties during normal or emergency operations.

(3) Diseases—Individuals shall have no established medical history or medical diagnosis of epilepsy or diabetes, or, where such a condition exists, the individual shall provide medical evidence that the condition can be controlled with proper medication so that the individual will not lapse into a coma or unconscious state while performing assigned security job duties.

(4) Addiction—Individuals shall have no established medical history or medical diagnosis of habitual alcoholism or drug addiction, or, where such a condition has existed, the individual shall provide certified documentation of having completed a rehabilitation program which would give a reasonable degree of confidence that the individual would be capable of performing assigned security job duties.

(5) Other physical requirements—An individual who has been incapacitated due to a serious illness, injury, disease, or operation, which could interfere with the effective

performance of assigned security job duties shall, prior to resumption of such duties, provide medical evidence of recovery and ability to perform such security job duties.

2. Mental qualifications: a. Individuals whose security tasks and job duties are directly associated with the effective implementation of the licensee physical security and contingency plans shall demonstrate mental alertness and the capability to exercise good judgment, implement instructions, assimilate assigned security tasks, and possess the acuity of senses and ability of expression sufficient to permit accurate communication by written, spoken, audible, visible, or other signals required by assigned job duties.

b. Armed individuals, and central alarm station operators, in addition to meeting the requirement stated in paragraph a. above, shall have no emotional instability that would interfere with the effective performance of assigned security job duties. The determination shall be made by a licensed psychologist or psychiatrist, or physician, or other person professionally trained to identify emotional instability.

c. The licensee shall arrange for continued observation of security personnel and for appropriate corrective measures by responsible supervisors for indications of emotional instability of individuals in the course of performing assigned security job duties. Identification of emotional instability by responsible supervisors shall be subject to verification by a licensed, trained person.

C. Medical examinations and physical fitness qualifications—Guards, armed response personnel, armed escorts and other armed security force members shall be given a medical examination including a determination and written certification by a licensed physician that there are no medical contraindications as disclosed by the medical examination to participation by the individual in physical fitness tests. Subsequent to this medical examination, guards, armed response personnel, armed escorts and other armed security force members shall demonstrate physical fitness for assigned security job duties by performing a practical physical exercise program within a specific time period. The exercise program performance objectives shall be described in

the license training and qualifications plan and shall consider job-related functions such as strenuous activity, physical exertion, levels of stress, and exposure to the elements as they pertain to each individual's assigned security job duties for both normal and emergency operations. The physical fitness qualification of each guard, armed response person, armed escort, and other security force member shall be documented by a licensee security supervisor or a qualified training instructor. The licensee shall retain this documentation as a record for three years from the date of each qualification.

D. Contract security personnel—Contract security personnel shall be required to meet the suitability, physical, and mental requirements as appropriate to their assigned security job duties in accordance with section I of this appendix.

E. Physical requalification—At least every 12 months, central alarm station operators shall be required to meet the physical requirements of B.1.b of this section, and guards, armed response personnel, and armed escorts shall be required to meet the physical requirements of paragraphs B.1.b (1) and (2), and C of this section. The licensee shall document each individual's physical requalification and shall retain this documentation of requalification as a record for three years from the date of each requalification.

F. Documentation—The results of suitability, physical, and mental qualifications data and test results must be documented by the licensee or the licensee's agent. The licensee or the agent shall retain this documentation as a record for three years from the date of obtaining and recording these results.

G. Nothing herein authorizes or requires a licensee to investigate into or judge the reading habits, political or religious beliefs, or attitudes on social, economic, or political issues of any person.

II. Training and qualifications.

A. Training requirements—Each individual who requires training to perform assigned security-related job tasks or job duties as identified in the licensee physical security or contingency plans shall, prior to assignment, be trained to perform these

tasks and duties in accordance with the licensee or the licensee's agent's documented training and qualifications plan. The licensee or the agent shall maintain documentation of the current plan and retain this documentation of the plan as a record for three years after the close of period for which the licensee possesses the special nuclear material under each license for which the plan was developed and, if any portion of the plan is superseded, retain the material that is superseded for three years after each change.

B. Qualification requirements—Each person who performs security-related job tasks or job duties required to implement the licensee physical security or contingency plan shall, prior to being assigned to these tasks or duties, be qualified in accordance with the licensee's NRC-approved training and qualifications plan. The qualifications of each individual must be documented by a qualified training instructor or a security supervisor. The licensee shall retain this documentation of each individual's qualifications as a record for three years after the employee ends employment in the security-related capacity and for three years after the close of period for which the licensee possesses the special nuclear material under each license, and superseded material for three years after each change.

C. Contract personnel—Contract personnel shall be trained, equipped, and qualified as appropriate to their assigned security-related job tasks or job duties, in accordance with sections II, III, IV, and V of this appendix. The qualifications of each individual must be documented by a qualified training instructor or a licensee security supervisor. The licensee shall retain this documentation of each individual's qualifications as a record for three years after the employee ends employment in the security-related capacity and for three years after the close of period for which the licensee possesses the special nuclear material under each license, and superseded material for three years after each change.

D. Security knowledge, skills, and abilities—Each individual assigned to perform the security related task identified in the licensee physical security or contingency plan shall demonstrate the required knowledge, skill, and ability in accordance with the

specified standards for each task as stated in the NRC approved licensee training and qualifications plan.

E. Requalification—Security personnel shall be requalified at least every 12 months to perform assigned security-related job tasks and duties for both normal and contingency operations. Requalification shall be in accordance with the NRC-approved licensee training and qualifications plan. The results of requalification must be documented and attested by a licensee security supervisor or a qualified training instructor. The licensee shall retain this documentation of each individual's requalification as a record for three years from the date of each requalification.

III. Weapons training.

A. Guards, armed response personnel and armed escorts requiring weapons training to perform assigned security related job tasks or job duties shall be trained in accordance with the licensees' documented weapons training programs. Each individual shall be proficient in the use of their assigned weapon(s) and shall meet licensee-prescribed standards for firearms handling and functionality.

IV. Weapons qualification and requalification program.

Qualification firing for the handgun and the rifle must be for daylight firing, and each individual shall perform night firing for familiarization with assigned weapon(s). The results of weapons qualification and requalification must be documented by the licensee or the licensee's agent. Each individual shall be requalified at least every 12 months. The licensee shall retain this documentation of each qualification and requalification as a record for three years from the date of the qualification or requalification, as appropriate.

A. Individuals shall qualify with all assigned firearms through completion of a law enforcement course or an equivalent nationally recognized course of fire.

B. 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. Enhanced weapons—Armed members of the security organization, assigned duties and responsibilities involving the use of enhanced weapons, authorized under § 73.15 of this part, must qualify in accordance with the licensee's NRC-approved training and qualification plan as specified under the provisions of § 73.15(f)(3) and (h) of this part.

D. Requalification—Individuals shall be weapons requalified at least every 12 months in accordance with the NRC approved licensee training and qualifications plan, and in accordance with the requirements stated in A, B, and C of this section.

V. Guard, armed response personnel, and armed escort equipment.

Fixed site guards, fixed site armed response personnel, and transportation armed escorts shall either be equipped with or have available the following security equipment appropriate to the individual's assigned contingency security related tasks or job duties as described in the licensee physical security and contingency plans:

A. Automatic or semiautomatic rifles.

B. 12 gauge shotguns.

C. Semiautomatic pistols or revolvers.

D. Short-barreled rifles.

E. Ammunition.

1. Each individual assigned contingency security job duties must maintain an adequate and readily available supply of ammunition for assigned weapons as determined by security job duties and responsibilities, as described in the licensee physical security and contingency plans.

2. The quantity of ammunition available for fixed sites must be maintained at a level sufficient to ensure the effective implementation of the Commission-approved security plans.

F. The licensee shall ensure that each individual is equipped or has readily available personal equipment or devices required for the effective implementation of the Commission-approved security plans.

G. Escort vehicles must be bullet resisting and equipped with communications systems or any other equipment as needed for the effective implementation of the Commission-approved security plans.

VI. Nuclear Power Reactor Training and Qualification Plan for Personnel Performing Security Program Duties

A. General Requirements and Introduction

1. The licensee must ensure that all individuals who are assigned duties and responsibilities required to implement the Commission-approved security plans, licensee response strategy, and implementing procedures, meet minimum training and qualification requirements to ensure each individual possesses the knowledge, skills, and abilities required to effectively perform the assigned duties and responsibilities.

2. Licensee physical protection programs that meet the requirements of 10 CFR 73.55(b)(3)(iii) must establish and maintain a training and qualification program that ensures personnel who are responsible for implementation of the physical protection of the facility against radiological sabotage are trained and qualified with the applicable portions of this section to effectively perform their assigned security-related job duties. The training and qualification program must be described in the Commission-approved training and qualification plan.

3. The licensee may not allow any individual to perform any security function, assume any security duties or responsibilities, or return to security duty, until that individual satisfies the training and qualification requirements of this appendix and the Commission-approved training and qualification plan, unless specifically authorized by the Commission.

4. Annual requirements must be scheduled at a nominal 12-month periodicity. Annual requirements may be completed up to 3 months before or 3 months after the scheduled date. However, the next annual training must be scheduled 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 serving in an armed capacity must not be disqualified from possessing or using firearms or ammunition in accordance with applicable state or Federal law, to include 18 U.S.C. 922. Licensees must use information that has been obtained during the completion of the individual's background investigation for unescorted access to determine suitability.

(b) The qualification of each individual to perform assigned duties and responsibilities must be documented and attested by a qualified training instructor or a security supervisor.

2. Physical qualifications.

(a) General physical qualifications.

(1) Individuals whose duties and responsibilities are directly associated with the effective implementation of the Commission-approved security plans, licensee protective strategy, and implementing procedures, may not have any physical conditions that would adversely affect their performance of assigned security duties and responsibilities.

(2) Armed and unarmed individuals assigned security duties and responsibilities must be subject to a physical examination designed to measure the individual's physical ability to perform assigned duties and responsibilities as identified in the Commission-approved security plans, licensee protective strategy, and implementing procedures.

(3) This physical examination must be administered by a licensed health professional with the final determination being made by a licensed physician to verify the individual's physical capability to perform assigned duties and responsibilities.

(4) The licensee must ensure that both armed and unarmed individuals who are assigned security duties and responsibilities identified in the Commission-approved security plans, the licensee protective strategy, and implementing procedures, meet the following minimum physical requirements, as required to effectively perform their assigned duties.

(b) 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 must 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.

(c) 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 must 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.

(d) 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 must, before resumption of assigned duties and responsibilities, provide medical evidence of recovery and ability to perform these duties and responsibilities.

3. Psychological qualifications.

(a) Armed and unarmed individuals must demonstrate the ability to apply good judgment, mental alertness, the capability to implement instructions and assigned tasks, and possess the acuity of senses and ability of expression sufficient to permit accurate communication by written, spoken, audible, visible, or other signals required by assigned duties and responsibilities.

(b) A licensed psychologist, psychiatrist, or physician trained in part to identify emotional instability must 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 must determine whether unarmed individuals in addition to meeting the requirement stated in paragraph (a) of this section, have no emotional instability that would interfere with the effective performance of assigned duties and responsibilities.

4. Medical examinations and physical fitness qualifications.

(a) Armed members of the security organization must be subject to a medical examination by a licensed physician, to determine the individual's fitness to participate in physical fitness tests.

(1) The licensee must 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.

(2) [Reserved]

(b) Before assignment, armed members of the security organization must demonstrate physical fitness for assigned duties and responsibilities by performing a practical physical fitness test.

(1) The physical fitness test must include physical attributes and performance objectives that demonstrate the strength, endurance, and agility, consistent with assigned duties in the Commission-approved security plans, licensee protective strategy, and implementing procedures during normal and emergency conditions.

(2) The licensee must describe the physical fitness test in the Commission-approved training and qualification plan.

(3) The physical fitness qualification of each armed member of the security organization must be documented and attested by a qualified training instructor or a security supervisor.

5. Physical requalification.

(a) At least annually, armed and unarmed individuals must be required to demonstrate the capability to meet the physical requirements of this appendix and the licensee training and qualification plan.

(b) The physical requalification of each armed and unarmed individual must be documented and attested by a qualified training instructor or a security supervisor.

C. Duty Training

1. On-the-job training.

(a) The licensee training and qualification program must include on-the-job training performance standards and criteria to ensure that each individual demonstrates the requisite knowledge, skills, and abilities needed to effectively carry-out assigned duties and responsibilities in accordance with the Commission-approved security plans, licensee protective strategy, and implementing procedures, before the individual is assigned the duty or responsibility.

(b) In addition to meeting the requirement stated in paragraph C.1.(a) of this appendix, before assignment, individuals (e.g., response team leaders, alarm station operators, armed responders, and armed security officers designated as a component of the protective strategy) assigned duties and responsibilities to implement the Safeguards Contingency Plan must complete on-the-job training to demonstrate their ability to effectively apply the knowledge, skills, and abilities required to effectively perform assigned *contingency* duties and responsibilities in accordance with the approved safeguards contingency plan, other security plans, licensee protective strategy, and implementing procedures. On-the-job training must be documented and attested by a qualified training instructor or a security supervisor.

2. Performance Evaluation Program.

(a) Licensees must develop, implement and maintain a Performance Evaluation Program that is documented in procedures which describes how the licensee will demonstrate and assess the effectiveness of their onsite physical protection program and protective strategy, including the capability of the armed response team to carry out

their assigned duties and responsibilities during safeguards contingency events. The Performance Evaluation Program and procedures must be referenced in the licensee's Training and Qualifications Plan.

(b) The Performance Evaluation Program must include procedures for the conduct of tactical response drills and force-on-force exercises designed to demonstrate and assess the effectiveness of the licensee's physical protection program, protective strategy and contingency event response by all individuals with responsibilities for implementing the safeguards contingency plan.

(c) The licensee must conduct tactical response drills and force-on-force exercises in accordance with Commission-approved security plans, licensee protective strategy, and implementing procedures.

(d) Tactical response drills and force-on-force exercises must be designed to challenge the site protective strategy against elements of the design basis threat and ensure each participant assigned security duties and responsibilities identified in the Commission-approved security plans, the licensee protective strategy, and implementing procedures demonstrate the requisite knowledge, skills, and abilities.

(e) Tactical response drills, force-on-force exercises, and associated contingency response training must be conducted under conditions that simulate, as closely as practicable, the site-specific conditions under which each member will, or may be, required to perform assigned duties and responsibilities.

(f) The scope of tactical response drills conducted for training purposes must be determined by the licensee and must address site-specific, individual or programmatic elements, and may be limited to specific portions of the site protective strategy.

(g) Each tactical response drill and force-on-force exercise must include a documented post-exercise critique in which participants identify failures, deficiencies or other findings in performance, plans, equipment or strategies.

(h) Licensees must document scenarios and participants for all tactical response drills and annual force-on-force exercises conducted.

(i) Findings, deficiencies and failures identified during tactical response drills and force-on-force exercises that adversely affect or decrease the effectiveness of the protective strategy and physical protection program must be addressed to ensure that timely corrections are made to the appropriate program areas.

(j) Findings, deficiencies and failures associated with the onsite physical protection program and protective strategy must be protected as necessary in accordance with the requirements of 10 CFR 73.21.

(k) For the purpose of tactical response drills and force-on-force exercises, licensees must:

(1) Use no more than the total number of armed responders and armed security officers documented in the security plans.

(2) Minimize the number and effects of artificialities associated with tactical response drills and force-on-force exercises.

(3) Implement the use of systems or methodologies that simulate the realities of armed engagement through visual and audible means or other technologies and reflect the capabilities of armed personnel to neutralize a target through the use of firearms.

(4) Ensure that each scenario used provides a credible, realistic challenge to the protective strategy and the capabilities of the security response organization.

(l) The Performance Evaluation Program must be designed to ensure that:

(1) Each member of each shift who is assigned duties and responsibilities required to implement the safeguards contingency plan and licensee protective strategy must participate in security drills and exercises.

(i) The licensee must conduct at least one fully integrated Force-on-Force exercise on an annual basis.

(ii) Each member of each shift must participate in one fully integrated Force-on-Force exercise every 3 years.

(iii) Each member of each shift must participate in two tactical response drills, one of which must be a limited scope tactical response drill, on an annual basis.

(A) Participation in a fully integrated Force-on-Force exercise or NRC triennial evaluation would count as credit for the limited scope tactical response drill. The NRC triennial evaluation can be used to satisfy the annual fully integrated Force-on-Force exercise.

(B) [Reserved]

(2) The mock adversary force replicates, as closely as possible, adversary characteristics and capabilities of the design basis threat described in 10 CFR 73.1(a)(1), and is capable of exploiting and challenging the licensee's protective strategy, personnel, command and control, and implementing procedures.

(3) Protective strategies can be evaluated and challenged through the conduct of tactical response tabletop demonstrations.

(4) Drill and exercise controllers are trained and qualified to ensure that each controller has the requisite knowledge and experience to control and evaluate exercises.

(5) Tactical response drills and force-on-force exercises are conducted safely and in accordance with site safety plans.

(m) Scenarios.

(1) Licensees must develop and document multiple scenarios for use in conducting tactical response drills and force-on-force exercises.

(2) Licensee scenarios must be designed to test and challenge any components or combination of components, of the onsite physical protection program and protective strategy.

(3) Each scenario must use a unique target set or target sets to ensure that the combination of all scenarios challenges every component of the onsite physical protection program and protective strategy to include, but not limited to, equipment, implementing procedures, and personnel.

D. Duty Qualification and Requalification

1. Qualification demonstration.

(a) Armed and unarmed individuals must demonstrate the required knowledge, skills, and abilities to carry out assigned duties and responsibilities as stated in the Commission-approved security plans, licensee protective strategy, and implementing procedures.

(b) [Reserved]

2. Requalification.

(a) Armed and unarmed individuals must 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 and attested by a qualified training instructor or a security supervisor.

E. Weapons Training

1. General firearms training.

(a) Armed members of the security organization must be trained and qualified in accordance with the requirements of this appendix and the Commission-approved training and qualification plan.

(b) Firearms instructors must maintain a certification for each weapon type from a national or state recognized entity.

(c) The Commission-approved training and qualification plan must describe training on firearms handling and functionality.

(d) The licensee must ensure that each armed member of the security organization is instructed on the use of deadly force as authorized by applicable State law.

F. Weapons Qualification and Requalification Program

1. General weapons qualification requirements.

(a) Qualification firing must be accomplished in accordance with Commission requirements and the Commission-approved training and qualification plan for assigned weapons.

(b) The results of weapons qualification and requalification must be documented and retained as a record.

2. Tactical weapons qualification. The licensee Training and Qualification Plan must describe the firearms used, the firearms qualification program, and other tactical training required to implement the Commission-approved security plans, licensee protective strategy, and implementing procedures. Licensee developed tactical qualification and requalification courses must describe the performance criteria needed to include the site specific conditions (such as lighting, elevation, fields-of-fire) under which assigned personnel must be required to carry-out their assigned duties.

3. Firearms qualification courses. The licensee must conduct the following qualification courses for each weapon used.

(a) Annual daylight qualification course. Qualifying score must be an accumulated total of 70 percent with handgun and shotgun, and 80 percent with 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.

(d) Individuals shall qualify with all assigned firearms through completion of a law enforcement course or an equivalent nationally recognized course of fire.

(e) Enhanced weapons. Armed members of the security organization, assigned duties and responsibilities involving the use of any weapon or weapons not described previously, must qualify in accordance with applicable standards established by a law enforcement course or an equivalent nationally recognized course for these weapons.

4. Firearms requalification.

(a) Armed members of the security organization must be requalified for each assigned weapon at least annually in accordance with Commission requirements and

the Commission-approved training and qualification plan, and the results documented and retained as a record.

(b) Firearms requalification must be conducted using the courses of fire outlined in paragraphs F.2 and F.3 of this section.

G. Weapons Maintenance

1. Firearms maintenance program. Each licensee must 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:

(a) Semiannual test firing for accuracy and functionality.

(b) Firearms maintenance procedures that include cleaning schedules and cleaning requirements.

(c) Program activity documentation.

(d) Control and accountability (weapons and ammunition).

(e) Firearm storage requirements.

(f) Armorer certification.

2. [Reserved]

H. Records

1. The licensee must retain all reports, records, or other documentation required by this appendix in accordance with the requirements of § 73.55(q).

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

3. The licensee must document data and test results from each individual's suitability, physical, and psychological qualification and must retain this documentation as a record for three (3) years from the date of obtaining and recording these results.

I. Reviews

The licensee must review the Commission-approved training and qualification program in accordance with the requirements of § 73.55(m).

J. Definitions

Terms defined in parts 50, 70, and 73 of this chapter have the same meaning when used in this appendix.

83. Revise and republish appendix C to part 73 to read as follows:

APPENDIX C TO PART 73—LICENSEE SAFEGUARDS CONTINGENCY PLANS

I. Safeguards Contingency Plan

Licensees, applicants, and certificate holders, with the exception of those who are subject to the requirements of § 73.55 or 73.100, must comply with the requirements of section I of this appendix.

A. Introduction

A licensee safeguards contingency plan is a documented plan to give guidance to licensee personnel in order to accomplish specific defined objectives in the event of threats, thefts, or radiological sabotage relating to special nuclear material or nuclear facilities licensed under the Atomic Energy Act of 1954, as amended. An acceptable safeguards contingency plan must contain:

1. A predetermined set of decisions and actions to satisfy stated objectives;

2. An identification of the data, criteria, procedures, and mechanisms necessary to efficiently implement the decisions; and

3. A stipulation of the individual, group, or organizational entity responsible for each decision and action.

The goals of licensee safeguards contingency plans for responding to threats, thefts, and radiological sabotage are:

1. To organize the response effort at the licensee level;

2. To provide predetermined, structured responses by licensees to safeguards contingencies;

3. To ensure the integration of the licensee response with the responses by other entities; and

4. To achieve a measurable performance in response capability.

Licensee safeguards contingency planning should result in organizing the licensee's resources in such a way that the participants will be identified, their several responsibilities specified, and the responses coordinated. The responses should be timely.

It is important to note that a licensee’s safeguards contingency plan is intended to be complementary to any onsite emergency plans.

B. Contents of the Plan

Each licensee safeguards contingency plan must include five categories of information:

1. Background

2. Generic Planning Base

3. Licensee Planning Base

4. Responsibility Matrix

5. Implementing Procedures

Although the implementing procedures (the fifth category of Plan information) are the culmination of the planning process, and therefore are an integral and important part of the safeguards contingency plan, they entail operating details subject to frequent changes. They need not be submitted to the Commission for approval, but will be inspected by NRC staff on a periodic basis. The licensee is responsible for ensuring that the implementing procedures reflect the information in the Responsibility Matrix, appropriately summarized and suitably presented for effective use by the responding entities.

The following paragraphs describe the contents of the safeguards contingency plan.

1. *Background.* Under the following topics, this category of information must identify and define the perceived dangers and incidents with which the plan will deal and the general way it will handle these:

a. Perceived Danger—A statement of the perceived danger to the security of special nuclear material, licensee personnel, and licensee property, including covert diversion of special nuclear material, radiological sabotage, and overt attacks. The statement of perceived danger should conform with that promulgated by the Nuclear Regulatory Commission. (The statement contained in 10 CFR 73.1 or subsequent Commission statements will suffice.)

b. Purpose of the Plan—A discussion of the general aims and operational concepts underlying implementation of the plan.

c. Scope of the Plan—A delineation of the types of incidents covered in the plan.

d. Definitions—A list of terms and their definitions used in describing operational and technical aspects of the plan.

2. *Generic Planning Base.* Under the following topics, this category of information must define the criteria for initiation and termination of responses to safeguards contingencies together with the specific decisions, actions, and supporting information needed to bring about such responses:

a. Identification of those events that will be used for signaling the beginning or aggravation of a safeguards contingency according to how they are perceived initially by licensee's personnel. Such events may include alarms or other indications signaling penetration of a protected area, vital area, or material access area; material control or material accounting indications of material missing or unaccounted for; or threat indications - either verbal, such as telephoned threats, or implied, such as escalating civil disturbances.

b. Definition of the specific objective to be accomplished relative to each identified event. The objective may be to obtain a level of awareness about the nature and severity of the safeguards contingency in order to prepare for further responses; to

establish a level of response preparedness; or to successfully nullify or reduce any adverse safeguards consequences arising from the contingency.

3. *Licensee Planning Base.* This category of information must include the factors affecting contingency planning that are specific for each facility or means of transportation. To the extent that the topics are treated in adequate detail in the licensee's approved physical security plan, they are not necessary to be repeated in this plan. The following topics should be addressed:

a. Licensee's Organizational Structure for Contingency Responses—A delineation of the organization's chain of command and delegation of authority as these apply to safeguards contingencies.

b. Physical Layout—(i) Fixed Sites—A description of the physical structures and their location on the site, and a description of the site in relation to nearby town, roads, and other environmental features important to the effective coordination of response operations. Particular emphasis should be placed on main and alternate entry routes for law-enforcement assistance forces and the location of control points for marshalling and coordinating response activities.

(ii) Transportation—A description of the vehicles, shipping routes, preplanned alternate routes, and related features.

c. Safeguards Systems Hardware—A description of the physical security and accounting system hardware that influence how the licensee will respond to an event. Examples of systems to be discussed are communications, alarms, locks, seals, area access, armaments, and surveillance.

d. Law Enforcement Assistance—A listing of available local law enforcement agencies and a description of their response capabilities and their criteria for response; and a discussion of working agreements or arrangements for communicating with these agencies.

e. Policy Constraints and Assumptions—A discussion of State laws, local ordinances, and company policies and practices that govern licensee response to incidents. Examples that may be discussed include:

(i) Use of deadly force;

(ii) Use of employee property;

(iii) Use of off-duty employees; and

(iv) Site security jurisdictional boundaries.

f. Administrative and Logistical Considerations—Descriptions of licensee practices that may have an influence on the response to safeguards contingency events. The considerations must include a description of the procedures that will be used for ensuring that all equipment needed to effect a successful response to a safeguards contingency will be easily accessible, in good working order, and in sufficient supply to provide redundancy in case of equipment failure.

4. *Responsibility Matrix.* This category of information consists of detailed identification of the organizational entities responsible for each decision and action associated with specific responses to safeguards contingencies. For each initiating event, a tabulation must be made for each response entity depicting the assignment of responsibilities for all decisions and actions to be taken in response to the initiating event. (Not all entities will have assigned responsibilities for any given initiating event.) The tabulations in the Responsibility Matrix must provide an overall picture of the response actions and their interrelationships. Safeguards responsibilities must be assigned in a manner that precludes conflict in duties or responsibilities that would prevent the execution of the plan in any safeguards contingency.

5. *Procedures.* In order to aid execution of the detailed plan as developed in the Responsibility Matrix, this category of information must detail the actions to be taken and decisions to be made by each member or unit of the organization as planned in the Responsibility Matrix.

C. Audit and Review

1. For nuclear facilities subject to the requirements of § 73.46, the licensee must provide for a review of the safeguards contingency plan at intervals not to exceed 24 months.

2. A licensee subject to the requirements of § 73.46 must ensure that the review of the safeguards contingency plan is by individuals independent of both security program management and personnel who have direct responsibility for implementation of the security program. The review must include an audit of safeguards contingency procedures and practices, and an audit of commitments established for response by local law enforcement authorities.

3. The licensee must document the results and the recommendations of the safeguards contingency plan review, management findings on whether the safeguards contingency plan is currently effective, and any actions taken as a result of recommendations from prior reviews in a report to the licensee's plant manager and to corporate management at least one level higher than that having responsibility for the day-to-day plant operation. The report must be maintained in an auditable form, available for inspection for a period of 3 years.

II. Nuclear Power Plant Safeguards Contingency Plans

A. Introduction

The safeguards contingency plan is a documented plan that describes how licensee personnel implement their physical protection program to defend against threats to their facility, up to and including the design basis threat of radiological sabotage.

Licensee safeguards contingency planning should result in organizing the licensee's resources in such a way that the participants will be identified, their responsibilities specified, and the responses coordinated. The responses should be timely and include personnel who are trained and qualified to respond in accordance with a documented training and qualification program.

The evaluation, validation, and testing of this portion of the program must be conducted in accordance with appendix B, section VI of this part, Nuclear Power Reactor Training and Qualification Plan for Personnel Performing Security Program Duties. The licensee's safeguards contingency plan is intended to maintain effectiveness during the implementation of onsite emergency plans.

B. Contents of the Plan

Each safeguards contingency plan must include five (5) categories of information:

(1) Background.

(2) Generic planning base.

(3) Licensee planning base.

(4) Responsibility matrix.

(5) Implementing procedures.

Although the implementing procedures (the fifth category of plan information) are the culmination of the planning process, and are an integral and important part of the safeguards contingency plan, they entail operating details subject to frequent changes. They need not be submitted to the Commission for approval, but are subject to inspection by NRC staff on a periodic basis.

1. Background. This category of information must identify the perceived dangers and incidents that the plan will address and a general description of how the response is organized.

a. Perceived Danger—Consistent with the design basis threat specified in § 73.1(a)(1), licensees must identify and describe the perceived dangers, threats, and incidents against which the safeguards contingency plan is designed to protect.

b. Purpose of the Plan—Licensees must describe the general goals, objectives and operational concepts underlying the implementation of the approved safeguards contingency plan.

c. Scope of the Plan—A delineation of the types of incidents covered by the plan.

(i) How the onsite or offsite response effort is organized and coordinated to effectively respond to a safeguards contingency event.

(ii) How the onsite or offsite response for safeguards contingency events has been integrated in other site emergency response procedures.

d. Definitions—A list of terms and their definitions used in describing operational and technical aspects of the approved safeguards contingency plan.

2. Generic Planning Base. Licensees must define the criteria for initiation and termination of responses to security events to include the specific decisions, actions, and supporting information needed to respond to each type of incident covered by the approved safeguards contingency plan. To achieve this result the generic planning base must:

a. Identify those events that will be used for signaling the beginning or aggravation of a safeguards contingency event according to how they are perceived initially by licensee's personnel. Licensees must ensure detection of unauthorized activities and must respond to all alarms or other indications signaling a security event, such as penetration of a protected area, vital area, or unauthorized barrier penetration (vehicle or personnel); tampering, bomb threats, or other threat warnings—either verbal, such as telephoned threats, or implied, such as escalating civil disturbances.

b. Define the specific objective to be accomplished relative to each identified safeguards contingency event. The objective may be to obtain a level of awareness about the nature and severity of the safeguards contingency to prepare for further responses; to establish a level of response preparedness; or to successfully nullify or reduce any adverse safeguards consequences arising from the contingency.

c. Identify the data, criteria, procedures, mechanisms and logistical support necessary to achieve the objectives identified.

3. Licensee Planning Base. This category of information must include factors affecting safeguards contingency planning that are specific for each facility. To the extent that the topics are treated in adequate detail in the licensee's approved physical

security plan, they may be incorporated by reference in the Safeguards Contingency Plan. The following topics must be addressed:

a. Organizational Structure. The safeguards contingency plan must describe the organization's chain of command and delegation of authority during safeguards contingency events, to include a general description of how command and control functions will be coordinated and maintained.

b. Physical Layout. The safeguards contingency plan must include a site map depicting the physical structures located on the site, including onsite independent spent fuel storage installations, and a description of the structures depicted on the map. Plans must also include a description and map of the site in relation to nearby towns, transportation routes (e.g., rail, water, and roads), pipelines, airports, hazardous material facilities, and pertinent environmental features that may have an effect upon coordination of response activities. Descriptions and maps must indicate main and alternate entry routes for law enforcement or other offsite response and support agencies and the location for marshaling and coordinating response activities.

c. Safeguards Systems. The safeguards contingency plan must include a description of the physical security systems that support and influence how the licensee will respond to an event in accordance with the design basis threat described in § 73.1(a). The licensee’s description must begin with onsite physical protection measures implemented at the outermost facility perimeter, and must move inward through those measures implemented to protect target set equipment.

(i) Physical security systems and security systems hardware to be discussed include security systems and measures that provide defense-in-depth, such as physical barriers, alarm systems, locks, area access, armaments, surveillance, and communications systems.

(ii) The specific structure of the security response organization to include the total number of armed responders and armed security officers documented in the approved

security plans as a component of the protective strategy and a general description of response capabilities must also be included in the safeguards contingency plan.

(iii) Armed responders must be available to respond from designated areas inside the protected area at all times and may not be assigned any other duties or responsibilities that could interfere with assigned armed response team duties and responsibilities.

(iv) Licensees must develop, implement, and maintain a written protective strategy to be documented in procedures that describe in detail the physical protection measures, security systems and deployment of the armed response team relative to site specific conditions, to include but not be limited to, facility layout, and the location of target set equipment and elements. The protective strategy should support the general goals, operational concepts, and performance objectives identified in the licensee's safeguards contingency plan. The protective strategy must:

(1) Be designed to meet the performance requirements and objectives of § 73.55(a) through (k) or 73.100(a) through (j), as applicable.

(2) Identify predetermined actions, areas of responsibility and timelines for the deployment of armed personnel.

(3) Contain measures that limit the exposure of security personnel to possible attack, including incorporation of bullet resisting protected positions.

(4) Contain a description of the physical security systems and measures that provide defense-in-depth, such as physical barriers, alarm systems, locks, area access, armaments, surveillance, and communications systems.

(5) Describe the specific structure and responsibilities of the armed response organization to include:

(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.

(iii) The total number of armed responders and armed security officers documented in the approved security plans as a component of the protective strategy.

(6) Provide a command and control structure, to include response by off-site law enforcement agencies, which ensures that decisions and actions are coordinated and communicated in a timely manner to facilitate response.

d. Law Enforcement Assistance. Provide a listing of available law enforcement agencies and a general description of their response capabilities and their criteria for response and a discussion of working agreements or arrangements for communicating with these agencies.

e. Policy Constraints and Assumptions. The safeguards contingency plan must contain a discussion of State laws, local ordinances, and company policies and practices that govern licensee response to incidents and must include, but is not limited to, the following.

(i) Use of deadly force.

(ii) Recall of off-duty employees.

(iii) Site jurisdictional boundaries.

(iv) Use of enhanced weapons, if applicable.

f. Administrative and Logistical Considerations. Descriptions of licensee practices which influence how the security organization responds to a safeguards contingency event to include, but not limited to, a description of the procedures that will be used for ensuring that equipment needed to facilitate response will be readily accessible, in good working order, and in sufficient supply.

4. Responsibility Matrix. This category of information consists of the detailed identification of responsibilities and specific actions to be taken by licensee organizations and/or personnel in response to safeguards contingency events.

a. Licensees must develop site procedures that consist of matrixes detailing the organization and/or personnel responsible for decisions and actions associated with

specific responses to safeguards contingency events. The responsibility matrix and procedures must be referenced in the licensee's safeguards contingency plan.

b. Responsibility matrix procedures must be based on the events outlined in the licensee's Generic Planning Base and must include the definition of the specific objective to be accomplished relative to each identified safeguards contingency event. The objective may be to obtain a level of awareness about the nature and severity of the safeguards contingency to prepare for further responses, to establish a level of response preparedness, or to successfully nullify or reduce any adverse safeguards consequences arising from the contingency.

c. Responsibilities must be assigned in a manner that precludes conflict of duties and responsibilities that would prevent the execution of the safeguards contingency plan and emergency response plans.

d. Licensees must ensure that predetermined actions can be completed under the postulated conditions.

5. Implementing Procedures. Licensees must establish and maintain written implementing procedures that provide specific guidance and operating details that identify the actions to be taken and decisions to be made by each member of the security organization who is assigned duties and responsibilities required for the effective implementation of the security plans and the site protective strategy.

C. Records and Reviews

1. Licensees must review the safeguards contingency plan in accordance with the requirements of § 73.55(m) or 73.100(f).

2. The safeguards contingency plan audit must include a review of applicable elements of the Physical Security Plan, Training and Qualification Plan, implementing procedures and practices, the site protective strategy, and response agreements made by local, State, and Federal law enforcement authorities.

3. Licensees must retain all reports, records, or other documentation required by this appendix in accordance with the requirements of § 73.55(q) or 73.100(j).

PART 95—FACILITY SECURITY CLEARANCE AND SAFEGUARDING OF NATIONAL SECURITY INFORMATION AND RESTRICTED DATA

84. The authority citation for part 95 continues to read as follows:

Authority: Atomic Energy Act of 1954, secs. 145, 161, 223, 234 (42 U.S.C. 2165, 2201, 2273, 2282); Energy Reorganization Act of 1974, sec. 201 (42 U.S.C. 5841); 44 U.S.C. 3504 note; E.O. 10865, as amended, 25 FR 1583, 3 CFR, 1959-1963 Comp., p. 398; E.O. 12829, 58 FR 3479, 3 CFR, 1993 Comp., p. 570; E.O. 12968, 60 FR 40245, 3 CFR, 1995 Comp., p. 391; E.O. 13526, 75 FR 707, 3 CFR, 2009 Comp., p. 298.

85. Revise § 95.1 to read as follows:

§ 95.1 Purpose.

The regulations in this part establish procedures for obtaining facility security clearance and for safeguarding Secret and Confidential National Security Information and Restricted Data received or developed in conjunction with activities licensed, certified or regulated by the Commission, in accordance with the National Industrial Security Program, as described in title 32 of the *Code of Federal Regulations* (32 CFR), part 117, “National Industrial Security Program Operating Manual (NISPOM).” This part does not apply to Top Secret information because Top Secret information may not be forwarded to licensees, certificate holders, or others within the scope of an NRC license or certificate.

86. In § 95.5:

a. In the definition “*Cognizant Security Agency (CSA)*”, remove the phrase “department of Energy” and add in its place the phrase “Department of Energy”; and

b. Add introductory text and remove the definitions of “*Combination lock*”, “*Need to know*”, “*Protective personnel*”, “*Restricted area*”, “*Security area*”, and “*Security container*”.

The additions read as follows:

§ 95.5 Definitions.

Terms defined in section 117.3 of title 32 have the same meaning when used in this part.

* * * * *

§ 95.8 [Amended]

87. In § 95.8, in paragraph (b):

a. Remove the references “95.18,” “95.25,” and “95.45,”; and

b. Add the reference “95.24,” in numerical order.

88. In § 95.11, revise the section heading and introductory text to read as follows:

§ 95.11 Specific exemptions and waivers.

The NRC may, upon application by any interested person or upon its own initiative, grant exemptions from the requirements of the regulations of this part, or waivers to the provisions of 32 CFR part 117 that are—

* * * * *

89. In § 95.17, revise the section heading and revise paragraph (a) to read as follows:

§ 95.17 Facility clearance process.

(a) Following the receipt of an acceptable request for facility clearance, the NRC will either accept an existing facility clearance granted by a current CSA and authorize possession of license or certificate related classified information, or process the facility for a facility clearance. Processing will include—

(1) A determination based on review and approval of a Standard Practice Procedures Plan that granting of the Facility Clearance would not be inconsistent with the national interest, including a finding that the facility is not under foreign ownership, control, or influence to such a degree that a determination could not be made. An NRC

finding of foreign ownership, control, or influence is based on factors concerning the foreign intelligence threat, risk of unauthorized technology transfer, type and sensitivity of the information that requires protection, the extent of foreign influence, record of compliance with pertinent laws, and the nature of international security and information exchange agreements.

(2) An acceptable operational readiness review conducted by the NRC;

(3) Submitting key management personnel, as defined in 32 CFR 117.7, for personnel clearances (PCLs); and

(4) Appointing a U.S. citizen employee as the facility security officer.

* * * * *

§ 95.18 [Reserved]

90. Remove and reserve § 95.18.

§ 95.19 [Amended]

91. In § 95.19, remove paragraph (c).

92. Add § 95.24 to read as follows:

§ 95.24 Safeguarding National Security Information and Restricted Data.

(a) Classified National Security Information and Restricted Data shall be protected in accordance with 32 CFR 117.15.

(b) Licensees will develop procedures for safeguarding National Security Information and Restricted Data in accordance with 32 CFR 117.7.

(c) Supervision of keys and padlocks. Use of key-operated padlocks are subject to the following requirements:

(1) A key and lock custodian shall be appointed to ensure proper custody and handling of keys and locks used for protection of classified matter;

(2) A key and lock control register must be maintained to identify keys for each lock and their current location and custody;

(3) Keys and locks must be audited each month;

(4) Keys must be inventoried with each change of custody;

(5) Keys must not be removed from the premises;

(6) Keys and spare locks must be protected equivalent to the level of classified matter involved;

(7) Locks must be changed or rotated at least every 12 months, and must be replaced after loss or compromise of their operable keys; and

(8) Master keys may not be made.

§ 95.25 [Reserved]

93. Remove and reserve § 95.25.

§ 95.27 [Reserved]

94. Remove and reserve § 95.27.

§ 95.29 [Reserved]

95. Remove and reserve § 95.29.

§ 95.31 [Reserved]

96. Remove and reserve § 95.31.

97. Revise § 95.33 to read as follows:

§ 95.33 Security training and briefings.

(a) Security training and briefings shall be conducted in accordance with 32 CFR 117.12.

(b) Records reflecting an individual’s initial and refresher security briefings and security terminations must be maintained for 3 years after termination of the individual’s access authorization.

98. Revise § 95.34 to read as follows:

§ 95.34 Visits and meetings.

Visits and meetings shall be conducted in accordance with 32 CFR 117.16.

§ 95.35 [Reserved]

99. Remove and reserve § 95.35.

100. Revise § 95.37 to read as follows:

§ 95.37 Classification and marking of documents.

(a) Documents shall be classified in accordance with 32 CFR 117.13.

(b) Classified documents shall be marked in accordance with 32 CFR 117.14.

101. Revise § 95.39 to read as follows:

§ 95.39 External transmission of documents and material.

Classified information shall be transmitted in accordance with 32 CFR 117.15(f).

102. Revise § 95.43 to read as follows:

§ 95.43 Reproduction of classified information.

Each licensee, certificate holder, or other person possessing classified information will follow the requirements established in 32 CFR 117.15(e)(6) for the reproduction of classified information.

§ 95.45 [Reserved]

103. Remove and reserve § 95.45.

104. Revise § 95.47 to read as follows:

§ 95.47 Destruction of matter containing classified information.

Each licensee, certificate holder, or other person possessing classified information will follow the requirements established in 32 CFR 117.15(g) for the destruction of classified information.

105. Revise § 95.49, to read as follows:

§ 95.49 Authorization to operate national security systems.

Classified data or information may not be stored, processed, or transmitted on information technology or operational technology systems without an authority to operate issued by the NRC authorization official for licensee classified systems based on 32 CFR 117.18, “Information system security.”

§ 95.51 [Reserved]

106. Remove and reserve § 95.51.

107. Revise § 95.57 to read as follows:

§ 95.57 Reports.

Each licensee, applicant for a license, certificate holder, construction-permit holder, or other person having a facility clearance must report to the NRC any incidents specified in 32 CFR 117.8. If the NRC is not the applicable CSA, then the licensee, applicant for a license, certificate holder, construction-permit holder, or other person must first report any incidents specified in 32 CFR 117.8 to their applicable CSA and then to the NRC.

(a) All actual or suspected losses or compromises of classified information must be reported to the NRC in accordance with the requirements set forth in 32 CFR 117.8(d). Initial reports, as prescribed in 32 CFR 117.8(d)(2), must be submitted to the NRC within the following timeframes:

(1) Confirmed or Suspected Compromise: If a loss, compromise, or suspected compromise is confirmed or reasonably suspected, an initial report must be submitted to

the NRC Headquarters Operations Center within 1 hour of discovery. A written confirmation of the incident must be submitted in accordance with § 95.9 of this part within forty-eight (48) hours of the event.

(2) No Compromise Determined: If it is determined that no loss, compromise, or suspected compromise occurred, a written report documenting this determination must be submitted in accordance with § 95.9 of this part within forty-eight (48) hours of reaching that conclusion.

(b) In addition, NRC requires records for all classification actions (documents classified, declassified, or downgraded) to be submitted to the NRC Division of Security Operations. These may be submitted either on an “as completed” basis or monthly. The information may be submitted either electronically by an on-line system (NRC prefers the use of a dial-in automated system connected to the Division of Security Operations) or by paper copy using NRC Form 790.

Dated: June 24, 2026.

For the Nuclear Regulatory Commission.

Tomas Herrera,
Acting Secretary of the Commission

[FR Doc. 2026-12989 Filed: 6/25/2026 8:45 am; Publication Date: 6/26/2026]