SUPPORTING STATEMENT1 FOR INFORMATION COLLECTIONS CONTAINED IN RISK-INFORMED, TECHNOLOGY-INCLUSIVE REGULATORY FRAMEWORK FOR ADVANCED REACTORS FINAL RULE

10 CFR PART 73
PHYSICAL PROTECTION OF PLANTS AND MATERIALS

(3150-0002)
REVISION

Description of the Information Collection

The U.S. Nuclear Regulatory Commission (NRC) is establishing an optional technology-inclusive regulatory framework for use by applicants for new commercial nuclear plant designs. The regulatory requirements developed in this rulemaking use methods of evaluation, including risk-informed and performance-based methods, that are flexible and practicable for application to a variety of new reactor technologies. The NRC's goals in amending these regulations are to continue to provide reasonable assurance of adequate protection of public health and safety and the common defense and security at reactor sites at which new nuclear reactor designs are deployed to at least the same degree of protection as required for current-generation light-water reactors; protect health and minimize danger to life or property to at least the same degree of protection as required for current-generation light-water reactors; provide greater operational flexibilities where supported by enhanced margins of safety that may be provided in new nuclear designs; and promote regulatory stability, predictability, and clarity.

The final rule covers a wide range of topics, including the following that result in recordkeeping and reporting requirements:

- Fitness for duty,
- Physical security,
- Cybersecurity,
- Access authorization.
- Plant design and analysis,
- Siting,
- Construction and manufacturing,
- Facility operations,
- Programs,
- Staffing,
- Decommissioning,
- Content of applications,
- Licensing basis information, and
- Quality assurance.

This supporting statement describes how the final rule impacts the information collections in 10 CFR Part 73 (3150-0002). 10 CFR 73.100 provides the performance objective and criteria for physical protection programs at 10 CFR Part 53 NRC-licensed nuclear power reactor facilities. Licensees complying with 10 CFR 73.100 must implement the requirements of the section through the physical security plan, training and qualification plan, safeguards contingency plan, and cybersecurity plan (the "security plans"), conduct performance reviews and audits,

implement corrective actions as necessary, and maintain records related to program implementation for inspection.

10 CFR 73.110 outlines additional requirements for the development of a cybersecurity program using a consequence-based approach. Under this requirement, licensees develop and maintain written policies, implementing procedures, and supporting technical information, which are subject to NRC inspection. In amended 10 CFR 73.77, the NRC added new notification requirements to ensure that potentially adverse cybersecurity events are escalated to senior management of the Part 53 facility, and to the NRC as necessary. These amendments are applicable to Part 53 licensees, and not to licensees under Parts 50 or 52.

Finally, 10 CFR 73.120 establishes information collection requirements related to access authorization programs for licensees subject to this section, including background checks of individuals who require unescorted access to the facility and reporting requirements for the behavioral observation program.

Accordingly, these sections introduce information collection requirements for applicants and licensees that elect to implement these sections as an alternative to the physical security requirements under 10 CFR 73.55, the cybersecurity requirements under 10 CFR 73.54, and the access authorization requirements under 10 CFR 73.55, 73.56, and 73.57.

Affected Entities

For the purposes of this supporting statement, the NRC staff estimates that there will be one respondent during the three-year period covered by this clearance (2027–2029). During this period, the NRC staff assumes that the respondent will be a holder of a combined license.

The information collection requirements under 10 CFR 73.100 are triggered for all Part 53 licensees that either: (1) demonstrate no achievable target sets exist in accordance with 10 CFR 73.100(b)(5) and credit active measures in making that determination, or (2) demonstrates achievable target sets exist in accordance with 10 CFR 73.100(b)(5). All Part 53 licensees that elect to implement 10 CFR 73.110 are also required to fulfill the information collection requirements associated with implementing a cybersecurity program. The holders of combined licenses and applicants for operating licenses under Part 53 that demonstrate compliance with 10 CFR 73.100(a)(1)(i) are subject to additional information collection requirements in connection with the access authorization program detailed in 10 CFR 73.120. Under the final rule, 10 CFR 73.77 is also amended to introduce information collection requirements for all Part 53 licensees upon the discovery of a cybersecurity event.

Information Collections

The Part 73 information collections imposed by the final rule are identified below by rulemaking topic. A more detailed description of the final rule changes is provided at the end of this supporting statement in “Description of Information Collection Requirements.”

- *Information about cyber events*. Reports of events having adverse consequences, or potentially adverse consequences, on the digital assets used to prevent fission product release and perform physical security functions.

- *Information about the physical security program*. Documents including a physical security plan, training and qualification plan, safeguards contingency plan, and

cybersecurity plan, and processes and procedures for implementing and evaluating these programs.

- *Information about the cybersecurity program.* Documents including written policies, implementing procedures, and supporting technical information, as well as program reviews.

- *Information related to the access authorization program*. Background investigations, signed consent forms, information connected to the behavioral observation program, self-reports of legal actions, access authorization lists, written notifications of unfavorable termination and denial of unescorted access, access authorization program reviews, and processes and procedures for determining trustworthiness for access determinations.

A. JUSTIFICATION

1. Need for the Collection of Information

The reporting and recordkeeping requirements in Part 73 are necessary for one or more of the following reasons:

- Information describing the content and planned operation of the licensee's physical protection system (e.g., cybersecurity plan, physical security plan, safeguards contingency plan, or training and qualification plan) is essential to enable the NRC to make a determination about the adequacy of the licensee's planned system in meeting regulatory requirements.

- Information describing the normal operation of the physical protection system (e.g., access authorizations) is needed to permit the NRC to make a determination as to reasonable assurance that the physical protection system operates in accordance with the regulatory requirements.

2. Agency Use and Practical Utility of Information

Applicants or licensees requesting approval to construct or operate commercial nuclear plants are required by the Atomic Energy Act of 1954, as amended (the Act), to provide information and data that the NRC may determine necessary to ensure the health and safety of the public.

The final rule requires licensees to maintain records related to the cybersecurity, physical security, and access authorization programs. Records related to the cybersecurity and physical security program must be maintained until the Commission terminates the license for which the records were developed and to maintain superseded portions of these records for at least three years after the record is superseded, unless otherwise specified by the Commission. Additionally, review and audit reports for the physical security program and, if any contracts exist to implement the program, the written agreement with the contractor, must be maintained for the duration specified in 10 CFR 73.100(j), as discussed in “Description of Information Collection Requirements.” Records related to the access authorization program must also be maintained for the duration specified in 10 CFR 73.120(c)(10), as discussed in “Description of Information Collection Requirements.”

Furthermore, licensees must report the suspension of security measures to the Commission.

This information will be used by the NRC to assess the adequacy of the licensee's plans to protect computer and communication systems and networks against cyberattacks, protect the plant against physical attacks, and ensure that unauthorized persons do not have access to the commercial nuclear plant, and that authorized persons are trustworthy and reliable.

3. Reduction of Burden Through Information Technology

The NRC has issued *Guidance for Electronic Submissions to the NRC*, which provides direction for the electronic transmission and submittal of documents to the NRC. Electronic transmission and submittal of documents can be accomplished via the following avenues: the Electronic Information Exchange (EIE) process, which is available from the NRC's "Electronic Submittals" Web page; by Optical Storage Media (OSM) (e.g., CD-ROM, DVD); by facsimile; or by e-mail.

The final rule does not impact the proportion of documents submitted to the NRC electronically. The percentage of electronic submission remains unchanged at 90 percent.

4. Effort to Identify Duplication and Use Similar Information

No sources of similar information are available. There is no duplication of requirements.

5. Effort to Reduce Small Business Burden

The NRC is currently not aware of any known small entities as defined in 10 CFR 2.810 that are planning to apply for a commercial nuclear plant early site permit, construction permit, operating license, manufacturing license, or combined license under Part 53 that will be impacted by this final rule.

6. Consequences to Federal Program or Policy Activities if the Collection Is Not Conducted or Is Conducted Less Frequently

Physical Security

In 10 CFR 73.100, the NRC requires licensees to maintain records related to the physical security program and report to the Commission the suspension of security measures. If the information were not collected, or were collected less frequently, the NRC would not have reasonable assurance that facilities are protecting health and safety or the common defense and security.

Cybersecurity

Revisions to 10 CFR 73.77 require Part 53 licensees to notify the NRC Headquarters Operations Center via the Emergency Notification System upon the discovery of cyber events with adverse, or potentially adverse, effects on the digital assets that perform important safety, security, and emergency preparedness functions at the facility. Additionally, 10 CFR 73.110 requires licensees to maintain records related to the cybersecurity program. If the information were not collected, or collected less frequently, the NRC would not have reasonable assurance that facilities are protected from cyberattacks.

Access Authorization

In 10 CFR 73.120, the NRC requires licensees to maintain records related to the access authorization program. If the information were not collected, or collected less frequently, the NRC would not have reasonable assurance that facilities are ensuring only trustworthy and reliable, authorized persons have access to the commercial nuclear plant.

7. Circumstances which Justify Variations from OMB Guidelines

Three requirements vary from the OMB provisions described in 5 CFR 1320.5(d)(2)(i) by requiring licensees and other entities to report information more than quarterly. These requirements, described below, ensure that that the NRC receives information in a timely manner so that it can assess and respond to the situation as needed:

- 10 CFR 73.77(a)(1) requires a Part 53 licensee to notify the NRC Headquarters Operations Center via the Emergency Notification System (ENS) within one hour of discovering a cyberattack that adversely impacted safety, security, or emergency preparedness functions, support systems and equipment, or security functions performed by digital assets to prevent a postulated fission product release or fulfill physical security requirements.
- 10 CFR 73.77(a)(2) requires a Part 53 licensee to notify the NRC Headquarter Operations Center via the ENS within four hours of discovering a cyberattack that could have adversely impacted safety, security, or emergency preparedness functions, support systems and equipment, or security functions performed by digital assets to prevent a postulated fission product release or fulfill physical security requirements. It also requires Part 53 licensees to submit a notification via the ENS within four hours of

discovering a suspected or actual cyberattack by personnel with physical or electronic access to digital computer and communication systems and networks within the scope of 10 CFR 73.54 or 10 CFR 73.110.

- 10 CFR 73.77(a)(3) requires a Part 53 licensee to notify the NRC Headquarter Operations Center via the ENS within eight hours of receiving or collecting information that may indicate intelligence gathering or pre-operational planning related to a cyberattack.

Five requirements vary from the OMB provisions described in 5 CFR 1320.5(d)(2)(iv) by requiring licensees and other entities to retain records for more than three years. These requirements, described below, ensure the availability of records for inspection, oversight, and regulatory proceedings:

- 10 CFR 73.100(b)(5) requires a Part 53 licensee to maintain site-specific analyses until submittal of the licensee's certifications required by 10 CFR 53.1070.
- 10 CFR 73.100 (j)(2) requires a Part 53 licensee to maintain all records that are required to be kept in accordance with Commission regulations, orders, or license conditions, until the Commission terminates the license for which the records were developed, and maintain superseded portions of these records for three years after the record is superseded, unless otherwise specified by the Commission.
- 10 CFR 73.100(j)(3) requires a Part 53 licensee that elects to implement the onsite physical protection program through the use of a contracted security force to retain a written agreement for the duration of the contract, which may exceed three years.
- 10 CFR 73.110(e)(5) requires Part 53 licensees to retain all records and supporting technical documentation required to demonstrate compliance with the requirements of 10 CFR 73.110 until license termination, and maintain portions of superseded records for three years afterward, unless otherwise specified by the Commission.
- 10 CFR 73.120(c)(10) requires documents regarding the trustworthiness and reliability of individual employees to be retained for three years from the date the individual no longer requires unescorted access. It also requires Part 53 licensees to retain access authorization program procedures for three years after the procedure is no longer needed and for superseded material to be retained for three years after it has been superseded. Finally, it requires Part 53 licensees to retain a list of persons approved for unescorted access for three years after the list is superseded or replaced.

One requirement varies from the OMB provisions described in 5 CFR 1320.5(d)(2)(ii) by requiring licensees and other entities to prepare a written response to a collection of information in fewer than 30 days after receipt:

- 10 CFR 73.77(b) requires Part 53 licensees to record vulnerabilities, weaknesses, failures, and deficiencies associated with their cybersecurity program in their site corrective action program within twenty-four hours of discovery. This requirement ensures that program issues are immediately incorporated into and addressed through the corrective action program.

8. Consultations Outside the NRC

The NRC published a proposed rule in the *Federal Register* for public comment on October 31, 2024 (89 FR 86918), as well as a draft OMB Supporting Statement for Part 73.

On November 19, 20, and 21, 2024, the NRC held a multi-day public meeting on the proposed rule. During this meeting, the NRC staff provided an overview of the proposed rule, addressed stakeholder questions, and communicated the methods available to submit public comments. The staff held a second public meeting on the proposed rule in early January 2025 with a focus on the topic of testing fueled manufactured reactors in the manufacturing facility and other technical topics of interest raised by stakeholders. In addition, the NRC staff hosted 24 public meetings with external stakeholders and participated in 16 Advisory Committee on Reactor Safeguards meetings on the draft proposed rule development before the rule was published for public comment.

The NRC prepared a summary and analysis of public comments received on the proposed rule and draft RGs, which totals two volumes (ML26042A229, ML26042A228). The public comment submissions are available from the Federal e-Rulemaking website at https://www.regulations.gov under Docket ID NRC-2019-0062.

As a result of the response to public comments, the NRC removed proposed 10 CFR 53.860(a)(2)(i) and (ii), which would have required an unmitigated consequence analysis using offsite dose reference values defined in 10 CFR 53.210 to demonstrate that the radiological sabotage design basis threat is not applicable, and instead moved the analysis requirement to 10 CFR 73.100 and provided licensees with a graded approach to implement requirements based on dose reference values defined in 10 CFR 53.210 that could credit mitigative actions, including shutting down the reactor. As a result, this supporting statement for the final rule includes two additional recordkeeping requirements:

- 10 CFR 73.100(b)(5) - Document the process used to identify achievable target sets, including the site-specific analyses and methodologies; implement a process for oversight of target set equipment and systems.
- 10 CFR 73.100(b)(5) - Maintain the process used to identify achievable target sets, including the site-specific analyses and methodologies; maintain records in accordance with 10 CFR 73.100(j); maintain site-specific analyses until submittal of the licensee's certifications required by 10 CFR 53.1070.

9. Payment or Gift to Respondents

Not applicable.

10. Confidentiality of Information

Confidential and proprietary information is protected in accordance with NRC regulations at 10 CFR 9.17(a) and 10 CFR 2.390(b). However, no information normally considered confidential or proprietary is requested.

Certain information designated as Safeguards Information is prohibited from public disclosure in accordance with the provisions of the Atomic Energy Act of 1954, as amended, Chapter 12, Section 147, or designated as classified National Security Information, in accordance with Executive Order 12958.

11. Justification for Sensitive Questions

Trade secrets, privileged, or confidential commercial or financial information is marked as proprietary information and is protected in accordance with NRC regulations in 10 CFR 9.17(a) and 10 CFR 2.390(b).

Certain information, designated as Safeguards Information (SGI), is prohibited from public disclosure in accordance with the provisions of the Atomic Energy Act of 1954, as amended, pursuant to Chapter 12, Section 147, or is designated as classified National Security Information, in accordance with Executive Order 12958, "Classified National Security Information," dated April 17, 1995.

For criminal history checks, the NRC collects fingerprints, either on hardcopy cards or electronically; digitizes fingerprints captured on cards; and passes the fingerprints electronically to the FBI. The FBI runs the fingerprints and provides the criminal history report to the NRC. The NRC passes this report on to the licensee without retaining a copy of it. This information collection is listed in the NRC's "Privacy Act of 1974; Republication of Systems of Records Notices," Volume 84 of the Federal Register, page 71536 (84 FR 71536, November 5, 2021), under the heading of NRC 39, "Personnel Security Files and Associated Records." The NRC does not disclose or share the information with anyone, except when initially submitting fingerprints to the FBI and when passing on the FBI report to the licensee.

12. Estimated Burden and Burden Hour Cost

Detailed burden estimates are included in the supplemental burden Excel spreadsheet titled, "Part 73 Burden Tables for the Part 53 Final Rule."

The NRC staff estimates that annually 1 licensee will be affected by the Part 73 collections during the period of this clearance.

The overall estimated annual burden is approximately 1,502.3 hours at an estimated annual cost of $231,354 (1,502.3 hours x $154/hour).

The NRC's average labor rate of $154 per hour for FY 2026 was used to calculate burden costs to the public because it aligns with 2024 Bureau of Labor Statistics data showing comparable hourly mean wages across five key occupational groups (executives, management, technical staff, licensing staff, and physicists) within the nuclear industry.

13. Estimate of Other Additional Costs

The quantity of records to be maintained is roughly proportional to the recordkeeping burden and therefore can be used to calculate approximate records storage costs. Based on the number of pages maintained for a typical clearance, the records storage cost has been determined to be equal to $0.12 per recordkeeping burden hour. Therefore, the storage cost for this clearance. as a result of this final rule is estimated to be $180 (1,502.3 recordkeeping hours x $0.12 per hour).

In addition, the current cost charged to licensees for processing fingerprint cards is $10 per card. The total cost for processing fingerprint cards is $502,550 (50,255 cards at $10 per card).

The total additional costs to licensees for the final rule is thus $502,826 ($180 + $502,550). The total additional costs for 10 CFR Part 73 information collections is $2,157,703 ($1,654,877 + $502,826).

14. Estimated Annualized Cost to the Federal Government

The final rule's changes to Part 73 are anticipated to affect one entity during the 3-year period covered by this supporting statement. The requirements under 10 CFR 73.100 provide for a performance-based approach to physical security, and licensee submissions are anticipated to require less time for NRC staff review than those submitted under 10 CFR 73.55 (which combine prescriptive and performance criteria). The following table identifies the reduced burden hours and costs for the NRC due to the final rule.

Annualized NRC Cost

NRC Action	Rule Text Provision	No. Actions / Year	Burden Hours / Action	Total Hours	Total Cost at $154/hour
Review records	73.100(b)(5), 73.100(c)(4), 73.100(f)(4), 73.100(j)(2)-(4), 73.110(e)(5), 73.120(c)(4) and (10)	1	-16	-16	-$2,464
Review processes and procedures	73.100(a)(1) 73.100(b)(8), 73.100(b)(9) 73.100(b)(10), 73.100(g)(2), 73.100(h)(4), 73.120(c)(10)	1	-16	-16	-$2,464
Review reports on suspension of security measures	73.100(i)(3)	0	-8	0	$0
Total		1	-32	-32	-$4,928

The staff has developed estimates of annualized costs to the Federal Government related to the conduct of this collection of information. These estimates are based on staff experience and subject matter expertise and include the burden needed to review, analyze, and process the collected information and any relevant operational expenses. The estimated annualized costs to the Federal Government are estimated to decrease by $4,928 due to the one Part 53 licensee during the clearance period (2027–2029).

The total costs to the Federal government for Part 73 information collections is $1,421,572 ($1,426,500 - $4,928).

15. Reasons for Changes in Burden or Cost

The estimated annual burden for information collection requirements for Part 73 is estimated to be 483,590 hours, an increase of 1,502.3 hours (482,088 hours + 1502.3 hours). The NRC staff anticipates that there will be one licensee under Part 53 in the period covered by this clearance.

The information collection is essential to permit NRC to make a determination as to the adequacy of the licensee's plans to protect computer and communication systems and networks against cyberattacks, protect the plant against physical attacks, and ensure that unauthorized persons do not have access to the commercial nuclear plant, and that authorized persons are trustworthy and reliable.

16. Publication for Statistical Use

The information being collected is not expected to be published for statistical use.

17. Reason for Not Displaying the Expiration Date

The recordkeeping and reporting requirements for this information collection are associated with regulations and are not submitted on instruments such as forms or surveys. For this reason, there are no data instruments on which to display an OMB expiration date. Further, amending the regulatory text of the CFR to display information that, in an annual publication, could become obsolete would be unduly burdensome and too difficult to keep current.

18. Exceptions to the Certification Statement

None.

B. COLLECTIONS OF INFORMATION EMPLOYING STATISTICAL METHODS

Not applicable.

DESCRIPTION OF INFORMATION COLLECTION REQUIREMENTS CONTAINED IN RISK-INFORMED, TECHNOLOGY-INCLUSIVE REGULATORY FRAMEWORK FOR ADVANCED REACTORS FINAL RULE
10 CFR PART 73

3150-0002

The Part 73 requirements that impose information collections are discussed below:

Section 73.77 establishes reporting and recordkeeping requirements for Part 53 licensees for cyber events.

- Section 73.77(a)(1) requires Part 53 licensees to notify the NRC Headquarters Operation Center via the Emergency Notification System within one hour of discovering a cyberattack that adversely impacted safety-related or important-to-safety functions, security functions, or emergency preparedness functions (including offsite communications); or that compromised support systems and equipment resulting in adverse impacts to safety, security, or emergency preparedness functions; or that adversely impacted (1) the safety, security, and emergency preparedness functions performed by digital assets to prevent a postulated fission product release that would result in offsite doses exceeding the values in 10 CFR 53.210, or (2) the security functions performed by digital assets necessary for implementing the physical security requirements in 10 CFR 53.860(a)(1).
- Section 73.77(a)(2) requires Part 53 licensees to notify the NRC Headquarters Operations Center within four hours of discovering a cyberattack that caused an adverse impact to safety-related or important-to-safety functions, security functions, or emergency preparedness functions (including offsite communications); or that could have compromised support systems and equipment, which if compromised, could have adversely impacted safety, security, or emergency preparedness functions; or could have caused an adverse impact to (1) the safety, security, and emergency preparedness functions performed by digital assets that prevent a postulated fission product release that would result in offsite doses exceeding the values in 10 CFR 53.210, or (2) security functions performed by digital assets necessary for implementing the physical security requirements in 10 CFR 53.860(a). Four-hour reports are also required for suspected or actual attacks by personnel with physical or electronic access to digital computer and communication systems and networks within the scope of § 73.54 or § 73.110.
- Section 73.77(a)(3) requires Part 53 licensees to notify the NRC Headquarters Operations Center within eight hours after receipt or collection of information regarding observed behavior, activities, or statements that may indicate intelligence gathering or pre-operational planning related to a cyberattack against digital computer and communication systems and networks within the scope of § 73.54 or § 73.110.
- Section 73.77(b) requires Part 53 licensees to record vulnerabilities, weaknesses, failures and deficiencies in their § 73.54 or § 73.110 cybersecurity program within twenty-four hours of their discovery.

Section 73.100 provides technology-inclusive requirements for physical protection of licensed activities at commercial nuclear plants against radiological sabotage.

- Section 73.100(a)(1) and (a)(2) provides the performance objective and criteria for physical protection programs at 10 CFR Part 53 NRC-licensed nuclear power reactor facilities. Licensees subject to 10 CFR 73.100 must implement the requirements of the section through its physical security plans, training and qualification plan, safeguards contingency plan, and cybersecurity plan, that each identify, describe, and account for site-specific conditions, prior to initial fuel load into the reactor (or for a fueled

manufactured reactor, before initiating the removal of the features to prevent criticality required under 10 CFR 53.620(d)(1)).

- Section 73.100(b)(1) requires licensees to establish, implement, and maintain a physical protection program and security organization that provides reasonable assurance that activities involving special nuclear material do not pose undue risk to common defense and security and public health and safety.
- Section 73.100(b)(5) requires licensees to perform a site-specific analysis to identify achievable target sets, document and maintain the process used to identify achievable target sets, including the site-specific analyses and methodologies used to determine and group the target set equipment or elements, implement a process for the oversight of target set equipment and systems, and maintain records in accordance with 10 CFR 73.100(j) and site-specific analyses until submittal of the licensee's certifications required by 10 CFR 53.1070.
- Section 73.100(b)(7) through (b)(11) requires licensees to establish, implement and maintain a performance evaluation program, access authorization program, cybersecurity program, and insider mitigation program, as well as a system to track trends and correct deficiencies in the implementation of these programs.
- Section 73.100(c)(2) requires the licensee's security organization to document security operations activities, security design and configuration controls, training and qualifications, and contingency responses.
- Section 73.100(c)(3) requires the licensee to establish a process for the head of the physical protection program to seek approval for changes in designs, policies, processes, and procedures and to ensure that these changes continue to satisfy the requirements for a physical protection program.
- Section 73.100(c)(4) requires the licensee to retain all analyses, assessments, calculations, and descriptions of the technical basis for meeting the requirements in Section 73.100(b) and protect safeguards information in accordance with 10 CFR 73.21 and 73.22.
- Section 73.100(e) requires licensees to establish and maintain a training and qualification program for personnel responsible for the physical protection of the facility.
- Section 73.100(f)(1) through (f)(4) requires licensees to establish and implement security reviews to evaluate the physical protection program. Paragraph (f)(1) requires licensees to identify and document vulnerabilities, improvements, and corrective actions related to engineered and administrative controls and the management systems used to implement the physical protection program. Paragraph (f)(2) requires licensees to perform self-assessments to ensure that capabilities to detect, assess, communicate, delay, interdict, and neutralize threats of radiological sabotage are effective, and perform design verification and assessments of the capabilities of active and passive engineering systems that protect against the design basis threat. Paragraph (f)(3) requires the security review to include several types of audits. Paragraph (f)(4) requires the licensee to maintain in a report the results and recommendations of onsite physical protection program reviews, management's finding regarding program effectiveness, and any actions taken as a result of recommendations from prior program reviews.
- Section 73.100(g)(1) and (g)(2) requires licensees to perform performance evaluations. Licensees will conduct performance evaluations at a frequency commensurate with the degree of security risk, document processes and procedures for implementing performance evaluations, verifications, and assessments, and maintain records related to the performance evaluations.
- Section 73.100(h)(4) requires licensees to document processes and procedures and maintain records for implementing corrective actions; compensatory measures; and maintenance, inspection, testing, and calibration of security structures, systems and equipment.
- Section 73.100(i)(3) requires licensees to report and document the suspension of security measures in accordance with 10 CFR 73.1200 and 73.1205.

- Sections 73.100(j)(2)-(4) requires licensees to maintain records until the Commission terminates the license for which the records were developed and maintain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the Commission. If a contracted security force is used to implement the onsite physical protection program, the rule requires licensees to maintain the licensee's written agreement with the contractor for the duration of the contract. The rule also requires licensees to maintain audit reports for inspection for 3 years.

Section 73.110 requires protection of digital computer and communication systems and networks.

- Section 73.110(a) requires Part 53 licensees to establish, implement, and maintain a cybersecurity program.
- Section 73.110(e)(2) requires the cybersecurity plan to account for site-specific conditions and describe the measures that are used to satisfy the requirements of 10 CFR 73.110.
- Section 73.110(e)(3) requires the licensee to develop and maintain written policies, implementing procedures, and other supporting technical information for the cybersecurity plan that may be subject to inspection by NRC staff.
- Section 73.110(e)(4) requires a review of the cybersecurity program as described in 10 CFR 73.100(f).
- Section 73.110(e)(5) requires the licensee to maintain all records and supporting technical documentation as a record until the Commission terminates the license and to maintain superseded portions of these records for at least three years after the record is superseded, unless otherwise specified by the Commission.

Section 73.120 establishes access authorization requirements.

- Section 73.120(a) requires licensees and applicants who demonstrate compliance with 10 CFR 73.100(a)(1)(i) to establish, maintain, and implement an access authorization program before initial fuel load into the reactor or initiating the removal of any one of the features to prevent criticality required under 10 CFR 53.620(d)(1) for a fueled manufactured reactor.
- Section 73.120(c)(1)(i)(A) requires licensees and applicants to conduct a background investigation of any individual seeking to obtain or maintain unescorted access to the facility.
- Section 73.120(c)(1)(i)(B) and (c)(1)(ii) requires background investigations to include the elements in 10 CFR 37.25, a credit history evaluation, fingerprinting, and an FBI identification and criminal history records check.
- Section 73.120(c)(1)(iii) requires licensees to obtain documented consent from the individual before initiating the background check.
- Section 73.120(c)(2)(i) requires a third-party disclosure, directing individuals who participate in the behavioral observation program to report information to the licensees or applicants when they observe actions or behaviors that may jeopardize health and safety.
- Section 73.120(c)(3) requires a third-party disclosure, requiring personnel with unescorted access to self-report to plant supervision any legal actions taken against them that could lead to incarceration or a court appearance, with the exception of minor civil actions or misdemeanors.
- Section 73.120(c)(4) requires the licensee pr applicant to maintain at all times a list of persons currently approved for unescorted access to a protected area, vital area, material access area, or controlled access area. Licensees and applicants will complete an FBI criminal history record check at least every ten years for each individual maintaining unescorted access.
- Section 73.120(c)(6)(ii) requires a third-party notification to individuals on the right to

complete, correct, or explain information obtained through the background investigation prior to any final adverse determination made by the licensee.

- Section 73.120(c)(7) requires licensees and applicants to document procedures for providing written notice to individuals who are denied unescorted access or unfavorably terminated.
- Section 73.120(c)(8) requires licensees, applicants, contractors, or vendors to implement a system of files and procedures to protect personal information against unauthorized disclosure.
- Section 73.120(c)(9) requires licensees and applicants to conduct a review of the access authorization program and the access authorization programs of contractors or vendors to document compliance with the requirements of 10 CFR 73.120.
- Section 73.120(c)(10) requires licensees, applicants, and contractors or vendors to document the processes and procedures for maintaining records used or created to establish an individual's trustworthiness and reliability or to document access determinations. Specifically, the following records are retained for the specified time periods: Documentation regarding the trustworthiness and reliability of individual employees for 3 years from the date the individual no longer requires unescorted access; a copy of the current access authorization program procedures for 3 years after the procedure is no longer needed, and if any portion of the procedure is superseded, the superseded material must be maintained for 3 years after the record is superseded; and the list of persons approved for unescorted access for 3 years after the list is superseded or replaced.