
INSPECTION PROCEDURE 81000 ATTACHMENT 12

CYBERSECURITY RESTART INSPECTION – PRE-FUEL LOAD

Effective Date: January 31, 2025

PROGRAM APPLICABILITY: IMC 2562

81000.12-01 INSPECTION OBJECTIVES

- 01.01 The objective of this procedure is to perform an initial evaluation of the cybersecurity program of nuclear power plants that have shut down, defueled, and permanently ceased operations under Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50 and then have decided to recommission the plant for commercial operations. This will be the first of two inspections with this inspection occurring prior to fuel load and the second inspection occurring after fuel load. This inspection is to verify the licensee's cybersecurity program is being properly reestablished to provide reasonable assurance that digital computer and communication systems and networks associated with safety, security, or emergency preparedness (SSEP) functions are adequately protected against cyberattacks in accordance with 10 CFR 73.54 and the licensee's U.S. Nuclear Regulatory Commission (NRC) approved cybersecurity plan (CSP).
- 01.02 To verify that the licensee has implemented provisions of the NRC approved CSP in accordance with the performance requirements specified by 10 CFR 73.55 (b)(8).
- 01.03 To verify the licensee's NRC approved CSP at the time of restart has been effectively maintained consistent with the licensing basis requirements.

81000.12-02 INSPECTION REQUIREMENTS

General Guidance

This inspection procedure (IP) was developed to verify the cybersecurity program established for implementation at a plant to be licensed or reestablishing a license in accordance with 10 CFR Part 50 or 10 CFR Part 52 appropriately meets NRC requirements and objectives for operational program cybersecurity readiness. Note that this inspection is conducted as licensees activate their operational program in accordance with IMC 2562, "Light-Water Reactor Inspection Program for Restart of Reactor Facilities Following Permanent Cessation of Power Operations." For restart of reactor facilities following termination of an operating license, this IP is applicable for transitioning from a decommissioned or extended shutdown reactor facility to an operational power reactor facility subject to the Reactor Oversight Process (ROP). Verification through observation of activities may not be possible. In such cases, the inspector(s) should review the appropriate licensee procedures and conduct inspections of associated areas to verify program compliance upon implementation.

Through completion of the inspection requirements within this IP, the inspector(s) can verify the licensee's cybersecurity program is designed and implemented to meet the general performance objectives of both its CSP and 10 CFR 73.55 (b)(8).

The inspector should consider the following inspection requirements in Sections 02.02 to 02.08 when developing the inspection plan and identifying the inspection sample.

Note: The paragraph references provided within parentheses after each inspection requirement below are from Nuclear Energy Institute (NEI) 08-09, "Cyber Security Plan for Nuclear Power Reactors," and NRC Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities." Both documents were determined by the NRC to be acceptable templates for developing the licensee's CSP.

02.01 Establishment of a Cybersecurity Assessment Team (CSAT)

- a. Verify the licensee has reestablished a CSAT and that the members are aware of and performing their duties and responsibilities. (NEI A.3.1.2, RG C.3.1.2)

Specific Guidance

The inspector(s) should review documentation to include, in part, letters of CSAT appointment, meeting notes, meeting minutes, implementing procedures, and license conditions. The inspector(s) should also consider conducting personnel interviews, and observing applicable CSAT licensee personnel, when possible, performing their duties to verify that the licensee has established its CSAT as described in the licensee's CSP.

- b. Verify that the CSAT is formed consisting of individuals with broad knowledge. (NEI (A.3.1.2) RG (C.3.1.2))

Specific Guidance

The broad knowledge required of the CSAT should be construed to mean in aggregate. The CSAT should include members from Information Technology, Operations, Maintenance, Engineering, Security, Emergency Preparedness, etc. An example of sources to verify the expertise and skill set of CSAT members may be licensee training records.

02.02 Identification and Documentation of Critical Systems (CS) and Critical Digital Assets (CDAs)

- a. Verify the licensee has appropriately identified SSEP CSs and CDAs. (NEI (A.3.1.3) RG (C.3.1.3))

Specific Guidance

To inspect this requirement, the inspector(s) should review documentation and implementing procedures, license conditions, and perform personnel interviews to verify the licensee has identified the SSEP CSs and CDAs that must be protected in accordance with the licensee's CSP and 10 CFR 73.54. A selected sample review of the licensee's identified SSEP CSs/CDAs is an appropriate scope for the inspector(s) to verify implementation of this requirement.

The inspector(s) should conduct a walkdown of at least one safety or security CS/CDA as part of the inspection of this requirement. Refer to the licensee's definition of a CS and CDA in the CSP.

The inspector(s) should randomly select at least two SSEP CSs/CDAs and review the documentation set consistent with the requirement.

02.03 Installation of a Protective Device between Lower and Higher Security Levels

- a. Verify the licensee has implemented the installation of a [deterministic one-way] boundary device between lower-level devices (Levels 0, 1, and 2) and the higher-level devices (Levels 3 and 4) as described in the Defense-in-Depth Protective Strategies. (NEI (A.4.3 and RG C.3.2))

Specific Guidance

The inspector(s) should review documentation, conduct personnel interviews, perform walkdowns, review network diagrams, review defense-in-depth design, and review implementing procedures, license conditions and requirements.

The inspector(s) should review the controls required by Defense-in-Depth (NEI E.6 and RG C.7) to verify that only one-way communication is allowed from the more secure levels to the less secure levels in accordance with NEI A.4.3 or RG C.3.2, unless specified differently in the licensing basis.

The inspector should verify that connections from the lower security levels cannot reach CDAs in the high security levels or that CDAs are not trying to reach and establish communication with other assets from the lower security levels.

02.04 Access Control/Portable Media and Device Protection

- a. Verify the licensee assesses attack vectors and access controls associated with portable media and mobile devices in accordance with the CSP. (NEI D.1.19 and RG B.1.19)

Specific Guidance

The inspector(s) should review documentation, perform personnel interviews and observation, review applicable training, and review the licensee's implementing procedures for the control and usage of portable media and mobile devices.

If possible, the inspector(s) should consider observing how access to portable media is controlled and how data is transferred from a lower security level to a higher security level (e.g. kiosk scanning, how virus signatures are updated, etc.).

02.05 Program Monitoring, Assessment, Configuration, and Change Management

- a. Verify the licensee has established a monitoring, assessment, configuration, and change management program in accordance with the CSP. (NEI (A.4.4, E.10) RG (A.4.1, C.11))

Specific Guidance

The inspector(s) should review a subset of the listed controls below, related to program monitoring, assessment, configuration, and change management, for the selected SSEP

CSs and CDAs samples and review how the licensee addresses those applicable controls. (NEI (A.3.1.4, A.4.4, A.4.4.3.1) RG (A.3.1.4, A.3.1.6, A.4.1, A.4.1.2))

- Configuration Management and Change Control, Configuration Management, and Configuration Change Control (NEI (A.4.4.1, E.10.1, E.10.4) RG (C.11.1, C.11.4, A.4.2.1))
- Configuration Management Policy and Procedures (NEI (E.10.2) RG (C.11.2))
- Baseline Configuration (NEI (E.10.3) RG (C.11.3))
- Installing Operating Systems, Applications, and Third-Party Software Updates (NEI (D.5.5) RG (B.5.5))
- Security Impact Analysis (NEI (A.4.4.2, E.10.5) RG (C.11.5))
- Flaw Remediation (NEI (E.3.2) RG (C.3.2))
- Access Restrictions for Change (Inspector(s) should consider support from contractors when inspecting this line item.) (NEI (E.10.6) RG (C.11.6))
- Security Functionality Verification (NEI (E.3.6) RG (C.3.6))
- Configuration Settings (Inspector(s) should consider support from contractors when inspecting this line item.) (NEI (E.10.7) RG (C.11.7))
- Evaluate and Manage Cyber Risk (NEI (E.12) RG (C.13.1))
- Ongoing Monitoring and Assessment (NEI (A.4.4) RG (C.4.1))

The inspector(s) should consider performing a walkdown of a selected sample of equipment to verify that the required baseline configuration documentation is correct and that any vulnerabilities identified have been remediated (if applicable).

02.06 Systems/Services Acquisition and Supply Chain Protection

- a. Verify the licensee addresses systems/services acquisition and supply chain protection controls in accordance with the CSP. (NEI (E.11) RG (C.12))

Specific Guidance

The inspector(s) should review procurement specifications, factory and site acceptance testing plans/results, in addition to appropriate references and documentation noted herein, to complete this inspection item.

The goal for this sample is to assess if the licensee is implementing a systems services and acquisition program for equipment that is being purchased and if that equipment is being received and stored correctly prior to installation in the plant. These requirements may also be applicable for CDAs that have been descoped and are being re-incorporated into the program. The controls listed below are, in part, related to systems/services acquisition and supply chain protection.

- System and Services Acquisition Policy and Procedures (NEI (E.11.1) RG (C.12.1))
- Supply Chain Protection (NEI (E.11.2) RG (C.12.2))
- Trustworthiness (NEI (E.11.3) RG (C.12.3))
- Integration of Security Capabilities (NEI (E.11.4) RG (C.12.4))
- Developer Security Testing (NEI (E.11.5) RG (C.12.5))
- Licensee Testing (NEI (E.11.6) RG (C.12.6))

02.07 Identification and Resolution of Problems

- a. Verify that the licensee is identifying issues related to the cybersecurity program at an appropriate threshold and entering them in the corrective action program. (NEI (A2.2.11) RG (A.4.3))
- b. Verify that the licensee has resolved the issues regarding regulatory requirements for a selected sample of problems associated with the cybersecurity program. Refer to IP 71152, "Problem Identification and Resolution (PI&R)," for additional guidance. (10 CFR 73.54(d)(2) and 10 CFR 73.55(b)(10))

Specific Guidance

The inspector(s) should review a sample of entries in the licensee's PI&R program associated with the cybersecurity program. The intent of this review is to verify that the licensee is identifying deficiencies at the appropriate threshold, tracking deficiencies for trending, and correcting deficiencies commensurate with their security significance. Inspector(s) can follow up on select samples, in accordance with this procedure, to ensure corrective actions are commensurate with the significance of the issue. Refer to IP 71152, Section 03.01, for additional guidance.

02.08 Review Changes to the CSP

- a. If changes to the CSP have been made, select a risk-informed sample to verify the licensee has performed an analysis as required by 10 CFR 50.54(p) and evaluate if the change(s) resulted in any decrease to the effectiveness of the commitments specified by CSP.

Specific Guidance

The inspector(s) should review a risk-informed sample of changes (based on their security significance) that have been made to the CSP to support pre-fuel activities and post-fuel inspection scope. The goal is to verify that those changes conformed accordingly to established regulatory requirements. Any selected changes made should be evaluated and compared to the NRC endorsed changes of NEI 08-09. The inspector may contact their CSB liaison in headquarters to obtain the latest information about changes to NEI 08-09 and to obtain clarification, as needed. If changes have been made to the CSP, the inspector(s) should verify that the change(s) did not result in a decrease in effectiveness of the CSP.

81000.12-03 INSPECTION GUIDANCE

General Guidance

This inspection encompasses a programmatic level review and verification of the licensee's implementation of a cybersecurity program. The references provided within parentheses after each inspection requirement below are from NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," and NRC RG 5.71, "Cyber Security Programs for Nuclear Facilities." Both documents were determined by the NRC to be acceptable templates for developing the licensee's CSP.

This inspection is expected to occur prior to fuel load; as such, it is recognized that the plant may have significant work in progress during this inspection. Therefore, the goal of this inspection is for the inspector(s) to be able to make an assessment that the licensee has procedures and processes in place that will enable them to successfully reestablish their cybersecurity program in accordance with their CSP.

The pre-fuel load inspection is designed to be completed in 1 week. The inspector(s) should look at how the SSEP CDAs that were not required to be operable when the plant was defueled are being reenrolled in the cybersecurity program. This part of the inspection should verify that the licensee has procedures to verify that the CDAs are properly reenrolled, their baseline configurations are updated, and known vulnerabilities are patched, mitigated, etc.

Because the scope of the cybersecurity program can be large, inspector(s) should request information in advance of the direct inspection effort. If inspector(s) elect to acquire this information remotely as opposed to in person, inspector(s) should use the document "Guidance Document for Development of the Request for Information (RFI) and Notification Letter for IP 71130.10, "Cyber Security." (Agencywide Documents Access and Management System (ADAMS) Accession No. [ML21330A088](#)).

The licensee's cybersecurity program will likely interface with many other plant operations and programs. As a result, if the inspector(s) conducting this IP identify a potential issue in another inspection area, that issue should be discussed with the cognizant branch chief responsible for that inspection area for resolution.

If findings and issues are identified relative to this IP, the inspector(s) should process them through the Security Issues Forum (SIF) to promote consistent application and resolution of inspection findings.

The cybersecurity controls (NEI (A.3.1.6) RG (A.3.1.6)) to mitigate cybersecurity risks are the technical, operational, and management countermeasures available to protect the availability, integrity, and confidentiality of CDAs.

Licensees may elect to implement the controls as specified, implement an alternative, or not implement (NEI (A.3.1.6) RG (A.3.1.6)). For situations in which an alternative control or security measure is provided as a substitute, the licensee should provide a documented basis that confirms the alternative control mitigates the threat/attack vector the original control is intended to protect and ensures that the functions of protected assets identified by 10 CFR 73.54(b)(1) are not adversely impacted due to cyberattacks. (NEI (A.3.1.6) RG (A.3.1.6))

For situations in which the applicant or licensee has determined to not implement a security control (e.g., the threat/attack vector addressed by the control does not exist), the licensee

should provide documentation that justifies why the control is not required; and demonstrate that the threat/attack vector does not exist. (NEI (A.3.1.6) RG (A.3.1.6))

If the licensee uses operator or manual actions to protect SSEP functions against a cyberattack, as an alternative countermeasure, these actions should be accomplished to prevent or mitigate adverse impact to SSEP functions. To determine effectiveness of implementation, the inspector(s) should consider the following:

- **Verification and Validation.** Determine whether the manual actions have been verified and validated by plant walkdowns using the licensee's most current procedure. Determine whether the licensee has adequately evaluated the capability of operators to perform the manual or operator action in the time available before the SSEP function will be placed in an unrecoverable condition.

Because the licensee will likely identify large numbers of CDAs, the inspection process should focus on digital SSEP CSs as opposed to individual digital components or system elements. A digital CS is a digital-technology-based system in or outside of the plant that performs or is associated with an SSEP function. These CSs include, but are not limited to, plant systems, equipment, communication systems, networks, offsite communications, or support systems or equipment, that perform or are associated with an SSEP function.

Inspector(s) may inspect entire CSs, portions of CSs, or CDAs which are part of SSEP CSs. When determining what portions of a CS to inspect, inspector(s) should choose a sample portion which is most representative of the licensee's cybersecurity program implementation.

The Commission in Staff Requirements Memorandum (SRM) COMWCO-10-0001, "Regulations of Cyber Security at Nuclear Power Plants," stated as a matter of policy that the NRC's cybersecurity rule, 10 CFR 73.54, should be interpreted to include structures, systems, and components in the balance of plant (BOP) that have a nexus to radiological health and safety at NRC licensed nuclear power plants. These systems would be considered important to safety. Inspector(s) should notify the Cyber Security Branch, Division of Physical and Cyber Security Policy, Office of Nuclear Security and Incident Response of any situations where any systems under Federal Energy Regulatory Commission regulatory oversight are controlled or secured by systems under NRC regulatory oversight. An example of this situation would be where a server inside the plant controls or secures a programmable logic controller, which is located at or beyond the first inter-tie in the switchyard.

81000.12-04 RESOURCE ESTIMATE

The estimated time to complete this IP is a direct inspection effort of 70 hours with a range of (60 to 80 hours) per site and will consist of approximately 1 week of direct inspection effort with subject matter expert (SME) support (if needed). This IP will be conducted as a team inspection. The team will generally consist of two regional inspectors. One SME may be added to the inspection at the discretion of the lead inspector. If an SME is added, the estimated time to complete the inspection will be 125 hours with a range of (120 to 128 hours).

81000.12-05 PROCEDURE COMPLETION

The inspectors should complete the requirements listed above (e.g. Sections 02.01 to 02.08) prior to fuel load, with the results informing the post-load requirement inspection activity. This IP

is not part of the baseline inspection program but is considered a prerequisite for the post-fuel load inspection.

The post-fuel load inspection is designed to be completed sometime after fuel load but prior to full power operation when the safety, important to safety, security, and EP CDAs are being inspected. Completion of the both the pre-fuel load and post-fuel load inspections will allow the Region to place the licensee back into the Cybersecurity Baseline inspection program.

81000.12-06 REFERENCES

10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks"

10 CFR 73.77, "Cyber Security Event Notifications"

Regulatory Guide (RG) 5.71, Rev. 0 "Cyber Security Programs for Nuclear Facilities"

RG 5.83, "Cyber Security Event Notifications" Site-specific Cyber Security Plan (CSP)

Site-specific Cyber Security Implementation Schedule NEI 08-09, Rev. 6, "Cyber Security Plan for Nuclear Power Reactors"

NEI 10-04, Revision 3, "Identifying Systems and Assets Subject to the Cyber Security Rule" and NRC Letter acknowledging NEI 10-04 to be acceptable for use with exceptions

NEI 13-10, Rev.7, "Cyber Security Control Assessments"

NEI 15-09, Revision 0, "Cyber Security Event Notifications" Security Frequently Asked Questions

END

Attachment 1: Revision History for 81000.12

Commitment Tracking Number	Accession Number Issue Date Change Notice	Description of Change	Description of Training Required and Completion Date	Comment Resolution and Closed Feedback Form Accession Number (Pre-Decisional, Non-Public Information)
N/A	ML24337A241 05/13/25 CN 25-011	First issuance. This is a one-time inspection of Palisades Nuclear Power Plant until December 31, 2027. It may be used in the future if another plant decides to restart after being permanently shut down and defueled.	None	ML24339A064