INSPECTION PROCEDURE 81000.13

CYBERSECURITY RESTART INSPECTION – POST-FUEL LOAD

Effective Date: January 1, 2026

PROGRAM APPLICABILITY: IMC 2562

CORNERSTONE: Security

This inspection procedure (IP) provides criteria that support re-establishing the baseline criteria for a facility seeking to return to operational status. The attributes to establishing these criteria are specified in Sections 03.01 – 03.03. Some of the applicable sections of this procedure may have been accomplished during the pre-fuel load IP 81000.12 and thus do not have to be reinspected. The inspection plan for IP 81000.12 will specify the sections that were inspected on the pre-fuel load inspection and do not need to be inspected by IP 81000.13 unless there have been changes since the IP 81000.12 inspection or deficiencies have been found in that section.

INSPECTION BASES: IMC 2562

SAMPLE REQUIREMENTS:

Sample Requirements		Minimum Baseline Sample Completion Requirements		Budgeted Range	
Sample Type	Section(s)	Frequency	Sample Size	*Samples	Hours
Cybersecurity – Post-fuel load	03.01 – 03.03	As applicable	4 Critical Systems	4 Critical Systems	140 +/- 7

The completion of all the requirements will constitute completion of the inspection sample. The inspector(s) will utilize insights obtained from the completed IP 81000.12, “Cybersecurity Restart Inspection – Pre-Fuel Load,” inspection and any operating experience within the respective fleet, as applicable, to inform the inspection activity. It is anticipated that at the time of this inspection activity, the licensee will have entered the Reactor Oversight Process (ROP). Final approval of the inspection scope will reside with the branch chief responsible for the inspection activity.

This inspection activity is to be conducted as necessary for plants in a decommissioned state and restarting. The anticipated duration of the inspection is 2 weeks. The team will select adequate Critical Digital Asset (CDA) samples from each of the CSs based on the size and complexity of the Critical System (CS).

81000.13-01 INSPECTION OBJECTIVES

01.01 To provide assurance the licensee's digital computer and communication systems and networks associated with safety, security, or emergency preparedness (SSEP) functions are adequately protected against cyberattacks in accordance with Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54 and the licensee's U.S. Nuclear Regulatory Commission (NRC) approved cybersecurity plan (CSP).

01.02 To verify that existing program CSP changes and reports are in accordance with 10 CFR 50 54(p).

81000.13-02 INSPECTION GUIDANCE

02.01 Background

For sites that are undergoing restart consistent with the IMC 2562 restart plan after being decommissioned, the evaluation of the cybersecurity program requirements occurs in two distinct phases. The first phase utilizes procedure IP 81000.12, "Cybersecurity Restart Inspection – Pre-Fuel Load." This procedure verifies the licensee performed the following:

- Establishment of a quality Cyber Security Assessment Team (CSAT);
- Identification and documentation of CSs and CDAs;
- Effectively implemented network architecture, established controls for management of portable media, mobile devices, and portable equipment (PMMD);
- Implemented program monitoring, assessment, configuration, and change management;
- Established systems/services acquisition and supply chain protection;
- Identification and resolution of problems; and
- addressed changes to the CSP.

The second phase of this inspection process utilizes the IP 81000.13, "Cybersecurity Restart Inspection – Post-Fuel Load," to ensure the licensee adequately meets the full-baseline requirements consistent with Part 50 and Part 52 facilities. Full implementation cybersecurity inspections (a.k.a., "Milestone 8 inspections") were conducted for the Part 50 and Part 52 facilities using IP 71130.10, "Cybersecurity." This IP was not part of the baseline but helped in establishing the baseline for subsequent procedures used for full implementation oversight activities. Prior to and during the full implementation inspections, additional guidance was developed and issued based on lessons learned from oversight program implementation. Nuclear Energy Institute (NEI) 13-10, "Cybersecurity Control Assessments," Revision 7, streamlined the process for addressing the application of cybersecurity controls to many CDAs. Industry issued addendums to NEI 08-09, "Cybersecurity Plan for Nuclear Power Reactors," Revision 6, to clarify the requirements for implementing controls while the NRC performed the full implementation inspections. In addition, industry continued efforts to clarify the process

for identification of digital assets identified as critical in the emergency planning and balance of plant areas, as the guidance in NEI 10-04, “Identifying Systems and Assets Subject to the Cybersecurity Rule,” and NEI 13-10 changed.

Throughout this procedure, the term “high assurance” is used in alignment with the Commission policy statement that high assurance is equivalent to reasonable assurance of adequate protection (NRC Staff Requirements Memorandum (SRM) SECY, “Options and Recommendations for the Force-On-Force Inspection Program in Response to SRM-SECY-14-0088,” Washington, DC, October 5, 2016 (Agencywide Documents Access Management System Accession No. ML16279A345)).

02.02 Guidance

All aspects of the licensee’s program are within the assessment scope of this inspection activity. Programmatic aspects the inspector(s) should focus on potentially include changes to the plant since the pre-fuel inspection activity, systems, structures, and components (SSCs) that have not been operating during the decommissioned period, and SSCs which have undergone restart implementation. CSs to review include, but are not limited to, plant systems, equipment, communication systems, networks, offsite communications, or support systems, or equipment that performs, or are associated with, SSEP functions. The inspector(s) should be sensitive to high functioning CDAs within CSs and CDAs that utilize software to accomplish SSEP and/or design basis functions. The inspector(s) can glean an understanding of these potential software updates by determining if there are any existing vulnerabilities listed within the National Vulnerability Database (NVD). A keyword search can be conducted by product or by common platform enumeration (CPE). If no changes have occurred through the design change process, safety/security interface requirements, or sourced via operating experience sources like the NVD, the inspector(s) will select four CSs, including at least one safety-related, one important-to-safety (ITS) system, and one security system, to review their current implementation.

Inspection findings and issues related to this IP shall be processed through the Security Issues Forum (SIF).

81000.13-03 INSPECTION REQUIREMENTS

General Guidance

This IP was developed to verify the cybersecurity program requirements for implementation at a plant reestablishing a license in accordance with 10 CFR Part 50 or 10 CFR Part 52. The inspection will assess if the entity appropriately meets NRC requirements and objectives for operational program cybersecurity readiness. Note that this inspection is conducted as licensees have loaded fuel to support 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 considered applicable for transitioning from a decommissioned or extended shutdown reactor facility to an operational power reactor facility subject to the ROP. Verification of inspection requirements through direct 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 that are observable to verify program compliance upon implementation.

The inspector(s) may want to consider reviewing any condition reports entered into the corrective action program (CAP) during the IP 81000.12, pre-fuel inspection to assist in ascertaining the effectiveness of the CAP program.

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(s) should consider the following inspection requirements in Sections 03.01 to 03.03 when developing the inspection plan and identifying the sample selections. Inspector(s) will select four CSs from safety, ITS, and security designators to perform inspection activities. These criteria are based on the 10 CFR 73.54 cybersecurity requirements encapsulating SSCs that are comprised of safety, ITS, security, and emergency preparedness. While the safety and ITS attributes can be quantified by various risk attributes, the security and emergency preparedness SSCs are attributes that warrant a different measure of assessment.

Risk-Informed Selection considerations:

Using the following consequence-based prioritization, inspectors should apply risk-informed considerations to refine the sample set. The following are additional attributes for consideration:

- Safety CDAs
- Boundary Devices (e.g., one-way deterministic data devices, firewalls)
- Monitoring, Detection or Protection Devices (e.g. SIEM, IDS, IPS, Scanning/Data Transfer stations)
- Important-to-Safety (ITS) CDAs
- Balance of Plant (BoP) CDAs
- DAs that provide protection or monitoring of CDAs

Note: The paragraph references provided with parentheses after each inspection requirement below are from 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 an acceptable template and either template can be used for developing the licensee's CSP.

03.01 Ongoing Monitoring and Assessment Activities

a. Review the process established by the licensee to conduct ongoing monitoring and assessments for CDAs. Verify that licensee procedures direct staff to conduct assessments or alternatives as required by the CSP. (NEI (4.4) RG (4.1))

Specific Guidance:

Ongoing monitoring and assessment activities are performed to verify that the cybersecurity controls implemented for CDAs remain in place. The monitoring and assessment activities are based on a representative sample of controls. Security assessments verify security-related activities and actions occur at the frequency

specified in security controls or within the evaluated alternate control frequency. Ongoing monitoring of cybersecurity controls used to support CDAs is implemented consistently with the licensee's CSP.

b. Verify that the licensee has established procedures that direct staff to conduct an appropriate effectiveness analysis as specified in the CSP. (NEI (4.4.3.1.1) RG (C.4.1.2))

Specific Guidance

The effectiveness analysis should include an evaluation of the cybersecurity program and the required controls, at least every 24 months or at the frequency specified in the CSP. The effectiveness analysis ensures that the cybersecurity controls are implemented correctly, operating as intended, and continue to provide high assurance that CDAs are protected against cyberattacks up to and including the design-basis threat (DBT). The analysis is based on a representative sample of CDAs, security controls, and program elements. Reviews of the cybersecurity program and controls include, but are not limited to, periodic audits of the physical security program, security plans, implementing procedures, cybersecurity programs, safety/security interface activities, and the testing, maintenance, and calibration program as it relates to cybersecurity.

c. Verify that the licensee has established a defensive architecture with the capabilities to detect, to respond to, and to recover from cyberattacks, as described by the CSP. (NEI (4.3) RG (3.1.5))

Specific Guidance

The licensee should have established defense-in-depth protective strategies specified in the CSP. Inspector(s) should verify they have been implemented, documented, and are maintained to ensure the licensee has the capability to detect, delay, respond to, and recover from cyberattacks on CDAs. These responses occur based on generated alarms due to potential cyber compromise, manual means of detection, or through the demonstration that a compromise can be detected along an attack pathway (e.g., wired, wireless, physical access, portable media, and supply chain testing).

d. Verify that the licensee has established controls and elements to ensure boundary protection for the cybersecurity levels and that integrity of data is maintained. (NEI (4.3) RG (C.3.2))

Specific Guidance

These protections can include host intrusion protection for devices and network intrusion detection/prevention for their network flows. Inspectors should determine if licensees have implemented and documented a multi-level security defensive architecture that establishes a required level of cybersecurity controls. The licensee may have separated their defensive levels by using security boundary devices, such as firewalls, air gaps, or deterministic devices, through which digital communications can be monitored, and restricted in accordance with CSP requirements. Systems requiring the greatest degree of security are located within the greatest number and strength of boundaries.

Inspectors should determine if the licensee has established or maintained procedures and processes, documented and implemented a defensive architecture to protect all

CDAs, systems, or equipment by verifying logical, and physical boundaries used to control the data transfer between boundaries and between devices.

e. Verify that the licensee has established or maintained security controls to provide high (reasonable) assurance that the CDAs are continuously protected against cyberattacks. (NEI (A.4.4) RG (C.3.3))

Specific Guidance

Inspectors should determine if the licensee has established procedures and processes to ensure cybersecurity risks are evaluated, managed, and mitigated to provide high assurance that digital computer and communication systems and networks are adequately protected against cyberattacks up to and including the DBT. Inspectors should confirm whether the licensee has established a process to verify and validate that the security controls implemented are operating as intended and are maintained consistently with the cybersecurity controls credited in the licensee's CSP. From the CDAs selected from the CS sample, inspector(s) should verify a sampling of CSP controls to ensure they are implemented in accordance with the CDA's assessment. Inspectors should verify the control is effective and meets the requirements set forth in the licensee's CSP.

f. Verify that the licensee has established access controls and authentication and user- identification capabilities. (NEI (D.1) RG (B.4))

Specific Guidance

The inspectors should determine if the licensee has established policies and procedures as required by the CSP. The licensee should be conducting reviews of their access authorization list. The inspector(s) can refer to the requirements specified in NEI 08-09, Appendix D, Section 4.2, "User Identification and Authentication" and its specific technical control attributes. The inspector(s)should also consider the applicability of the requirements of 10 CFR 73.56 (i)(1)(v)(B)(4) when verifying if individuals are trustworthy and reliable to implement the respective CSP.

03.02 Configuration Management and Change Control

a. Verify the licensee evaluates modifications to CDAs prior to implementation to assure that digital computer and communications systems and networks are adequately protected against cyberattacks. (NEI (A.4.5, E.10) RG (C.4.2))

Specific Guidance

The inspector(s) should determine if licensees are implementing this activity consistent with the performance requirements specified in the CSP and as applicable, NEI 08-09, Section 2.2.1, which states in part that modifications to CDAs will be evaluated prior to implementation to achieve high assurance that digital computer and communications systems and networks are adequately protected. These evaluations are typically performed as part of the licensee's configuration management program with oversight by the Cybersecurity Assessment Team (CSAT), so that additional cybersecurity risks are not introduced into the system. The inspectors should verify that implemented controls meet the requirements in the CSP.

b. Verify that the licensee performs a security impact analysis prior to making changes to CDAs to manage the cyber risk resulting from the changes.

Specific Guidance

A cybersecurity impact analysis is performed prior to making a design or configuration change to a CDA, or when changes to the environment occur. These changes can occur consistently with the attributes described in NEI 08-09, Appendix D, Section 5.5, "Installing Operating Systems, Applications, and Third-Party Software Update." The licensee evaluates changes to the required controls based on the assessment of the changes to manage risks introduced by the changes. The licensee assesses the interdependencies of other CDAs or support systems and incorporates the assessment into the cybersecurity impact analysis. (NEI A.4.4.2, E.10.5, RG C.11.5)

03.03 Cybersecurity Programmatic reviews

a. Determine if the licensee has made any changes to the CSP not inspected during the inspection activities of IP 81000.12, "Cybersecurity Inspection Pre – Fuel Load" to ensure the changes did not reduce the effectiveness of the plan. Verify that the licensee performed these activities in accordance with their cybersecurity program implementing procedures and NRC requirements. (NEI 2.2.7, A.3.1, RG C.4.2)

Specific Guidance

The licensee should have changed control procedures as well as licensing basis administrative controls for making changes to their CSP. The licensee can make changes to the CSP based on the requirements of 10 CFR 50.54(p). Further, the CSP requires that the licensee develop implementing procedures. Inspectors may want to leverage the process utilized to support the 10 CFR 50.71(e) requirements which are used to support changes made by the licensee to be included in the Updated Final Safety Analysis Report (UFSAR) revision.

b. Verify the licensee established an incident response process, including contingency plans, procedures, and notifications. (NEI A.4.6, RG C.3.3.2.6)

Specific Guidance

Inspectors should determine whether attributes reflect the identification, detection, and response to cyberattacks and are directed by site procedures that govern responses to plant events. Inspectors should assess when there is reasonable suspicion of a cyberattack, procedures direct notification to responsible individuals and activation of the Cybersecurity Incident Response Team, as well as other emergency response actions, if warranted. Inspectors should ensure the licensee has established procedures for testing the incident response capabilities at an interval of at least every 12 months or that consistent with their CSP.

If a cybersecurity incident occurred, ensure that the licensee took effective actions to ensure that the functions of CDAs are not adversely impacted and that the licensee implemented appropriate corrective actions.

The inspector(s) may observe a licensee-conducted Cybersecurity Incident Response drill if the licensee is performing a drill. If a drill does not occur, the Inspector(s) may consider interviews and/or tabletop scenarios with licensee personnel. The Inspector(s) should ensure the licensee has included the Cyber Security Contingency Plan (Continuity of Operations) as an attribute of the overall Physical Security Plan. 10 CFR 73.55(a)(1) requires that licensees implement the requirements of the section through its Commission-approved Physical Security plan, Training and Qualification plan, Safeguards Contingency plans, and Cyber Security plan, referred to collectively as "security plans."

c. Verify that the licensee has established training as described in the CSP. (NEI A.4.8, RG C.3.3.2.8)

Specific Guidance

Verify the licensee has established, implemented, documented, and is conducting or has conducted cyber training requirements for licensee personnel and contractors to perform their assigned duties and responsibilities in implementing the requirements of their cyber program. Inspectors should review licensee procedures, cybersecurity training completed from personnel training records, and conduct personnel interviews when observation of activities are not possible. These reviews should include subject matter experts of personnel responsible for implementation/maintaining of the CDAs selected in the inspection sample. The inspectors should verify the licensee has established a training curriculum to include general awareness, technical, specialized, and situational awareness training to support samples selected for review.

81000.13-04 RESOURCE ESTIMATE

The estimated time to complete the inspection procedure's direct inspection effort is 140 hours (with a range of 133 to 147 hours) per site and will consist of 2 weeks of direct inspection effort with contractor support. This inspection is planned to be conducted as a team inspection. The team shall consist of two regional inspectors and two contractors.

81000.13-05 PROCEDURE COMPLETION

The completion of all the requirements will constitute completion of the inspection sample. The inspector(s) will utilize insights from the IP 81000.12 inspection and operating experience within the fleet as applicable to inform the inspection. It is anticipated that at the time of this inspection activity, the licensee will have entered the ROP. Final approval of the inspection scope will reside with the branch chief responsible for the inspection.

The completion of the IP 81000.12 and IP 81000.13 should serve as an adequate basis for inspection activities conducted using the 71130.10 baseline cybersecurity procedures.

81000.13-06 REFERENCES

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

10 CFR 73.77, "Cyber security event notifications"

Regulatory Guide 5.71, “Cybersecurity Programs for Nuclear Facilities” (ML090340159) (Package ML090340152)

CYBERSECURITY: Guidance Document for Development of the Request for Information (RFI) and Notification Letter for Full Implementation of the Cybersecurity Inspection (ML21330A088)

Site’s NRC approved Cybersecurity Plan

NEI 08-09, “Cybersecurity Plan for Nuclear Power Reactors,” Revision 6, (ML101180437); Addendum 1 (ML17079A379); Addendum 2 (ML17212A634); Addendum 3 (ML17237C076);

Addendum 4, (ML17212A635), Addendum 5 (ML18226A007), Addendum 7 (ML18348B211)

NEI 10-04, “Identifying Systems and Assets Subject to the Cybersecurity Rule,” Revision 2, and NRC Letter acknowledging NEI 10-04 to be acceptable for use with exceptions (ML12180A081)

NEI 13-10, “Cybersecurity Control Assessments,” (Revision 6, ML17234A615); (Revision 5, ML17046A658); (Revision 4, ML15338A276); (Revision 3, ML15247A140); (Revision 2, ML14351A288); (Revision 1, ML14279A222); (Revision 0, ML14034A076)

Response to NEI White Paper, “Changes to NEI 10-04 and NEI 13-10, “Guidance for Identifying and Protecting Digital Assets Associated with Emergency Preparedness Functions,” Dated March 2020 - Final Copy (ML20126G492)

Response to NEI White Paper, “Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and protecting Digital Assets Associated with the Balance of Plant,” Dated July 2020,” (ML20205L604), issued August 14, 2020 (ML20209A442)

Security Frequently Asked Questions (SFAQ)

SFAQ	Title	Accession #
10-05	IT Functions for the Critical Group	ML102100070
10-06 12-17	Classification of Cyber Security Information Cybersecurity Milestone 1	ML102090633 ML13098A153
12-18	Cybersecurity Milestone 2	ML13098A155
12-19	Cybersecurity Milestone 3	ML13098A157
12-20	Cybersecurity Milestone 4	ML13098A170
12-21	Cybersecurity Milestone 5	ML12331A131
12-22	Cybersecurity Milestone 6	ML13098A174
12-23	Cybersecurity Milestone 7	ML13098A177
14-01	Digital Indicator, Rev. 1	ML15029A517
14-02 16-01	Unauthorized Person Data Integrity	ML16088A242 ML16196A302
16-02	Deterministic Devices	ML16208A222

SFAQ	Title	Accession #
16-03	Treatment of Digital Maintenance and Test Equipment	ML16350A056
16-04	Access Authorization/Personnel Access Data System	ML16209A095
16-05	Moving Data between Security Levels	ML16351A469
16-06	Communications Attack Pathways	ML16351A504
17-04	Access Authorization/Access Authorization Systems	ML18030A535

Response to NEI White Paper, “Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets associated with Safety-Related and Important- to-Safety Functions,” Dated July 2020 (ML20199M368)

Response to NEI White Paper, “Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Security,” Dated June 2021 (ML21140A140)

NEI 15-09, “Cybersecurity Event Notifications,” (Revision 0, ML16063A063)

Power Point Presentation describing the inspection and development history of cybersecurity (ML20324A636) SFAQ. The SFAQ are considered “For Official Use Only – Security-Related Information” and are available, upon request, to stakeholders with appropriate need to know.

END

Attachment 1: Revision History for IP 81000.13

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	ML25191A026 12/16/25 CN 25-034	First issuance. This is a program inspection to support post ROP start-up of a 10 CFR Part 50 facility that has been in a decommissioned state.	None	ML25254A220