
INSPECTION PROCEDURE 75100 ATTACHMENT 15

CYBERSECURITY INSPECTION DURING CONSTRUCTION OF ADVANCED REACTORS: PRE-OPERATIONS

Effective Date: 10/20/2026

PROGRAM APPLICABILITY: IMC 2203

STRATEGIC PERFORMANCE AREA: Security and Safeguards

75100.15-01 INSPECTION OBJECTIVES

- 01.01 To provide assurance that the cybersecurity program has been fully implemented in accordance with the regulatory requirements and the U.S. Nuclear Regulatory Commission (NRC) approved cybersecurity plan (CSP) prior to operations.
- 01.02 To ensure that the cybersecurity program has been properly implemented to provide reasonable assurance that digital computer and communication systems and networks associated with safety, security, and emergency preparedness (SSEP) functions are adequately protected against cyberattacks in accordance with the NRC-approved CSP.

75100.15-02 INSPECTION REQUIREMENTS

General Guidance

This inspection procedure (IP) works in conjunction with IP 75100.09, "Cybersecurity During Construction of Advanced Reactors: Pre-Fuel Arrival." This inspection should be conducted late in the construction period for advanced reactors such that the final configuration of systems and components can be verified and the applicant or licensee has their cybersecurity program in place. This IP is applicable to all advanced reactors under construction that are subject to oversight under the NRC's Advanced Reactor Construction Oversight Program (ARCOP). Verification through observation of activities may not be possible for all requirements. In such cases, the inspector(s) may review the appropriate permit or license holder's procedures and records.

Since advanced reactors will vary in design and licensing approaches, inspections will also be tailored to each site. The scope of inspections for advanced reactors will depend on the specific licensing framework and licensing basis selected by each permit or license holder. Therefore, some elements of this inspection procedure (IP) may be omitted. Additionally, many advanced reactors may be co-located with existing, operating reactors. Inspections of new reactors that use elements of existing site security plans do not need to include those elements that are the same as the operating reactors. For example, fitness-for-duty, access authorization, and safeguards information are areas where the NRC expects security plans to be essentially unchanged from the operating reactors' security plan. Any inspection activities that do not align with the permit or license holder's licensing and design basis should not be inspected.

This inspection includes a programmatic level review and verification of the adequate completion of requirements. The paragraph references provided within parentheses after each inspection requirement below are from guidance published by Nuclear Energy Institute (NEI) 08-09, and Regulatory Guide (RG) 5.71. Both documents were determined by the NRC staff to be acceptable for developing a CSP and for cybersecurity program implementation

Alternative controls may be implemented; inspectors must review the technical justification to confirm the alternate control addresses the attack vector the specified control is intended to address. For situations where it has been determined the control to be unnecessary (e.g., the attack vector addressed by the control does not exist), documentation is required to justify why the control is not required; and to demonstrate that the attack vector does not exist. (NEI (A.3.1.6) RG (A.3.1.6)).

A large number of critical digital assets (CDAs) may be identified. The inspection scope should focus on digital critical systems (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) should also note, relative to balance of plant (BOP) CSs/CDAs, “The Commission has determined as a matter of policy that the NRC’s cybersecurity rule at 10 CFR 73.54 should be interpreted to include structures, systems, and components in the BOP that have a nexus to radiological health and safety at NRC-licensed nuclear power plants.” Inspector(s) should notify the Cybersecurity Branch, Branch, NRR and OAR/AROB of any situations where any systems under Federal Energy Regulatory Commission (FERC) regulatory oversight are controlled or secured by systems under the 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.

Sample selection shall be consequence-based, risk-informed, scalable and shall focus on structures, systems, and components (SSCs) that support safety and security functions.

Inspector(s) shall select samples that enable fulfillment of the inspection procedure objectives, while prioritizing based on consequence, applying risk-informed insights, and scaling appropriately to the design under review.

Consequence-Based Selection considerations:

The consequence of a Critical Digital Asset (CDA) being unavailable is closely aligned with the safety significance of the SSC it supports but most likely can’t be quantified by some element of risk.

CDA Consequence Priority (Highest to Lowest):

- Boundary Devices (e.g., PMMDs, one-way deterministic data devices)
- Monitoring, Detection or Protection Devices (e.g. SEIM, IDS, IPS)
- Safety CDAs
- Security CDAs

- Important-to-Safety (ITS) CDAs
- Emergency Preparedness (EP) CDAs
- Balance of Plant (BOP) CDAs
- Non-Critical Digital Assets (DAs)

Sample selection should focus inspection on high-consequence CDAs (Boundary, Monitoring, Detection, Protection, Safety, Security). Only include moderate-consequence CDAs (EP and ITS) if necessary because limited high-consequence CDAs are available for inspection. Exclude low-consequence CDAs (BOP and DAs).

Note: The paragraph references provided within parentheses for applicable sections below are based on 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 a permit or license holder's CSP.

Risk-Informed Selection Considerations:

Boundary devices should always be inspected

When reviewing the potential CDAs for selection, additional risk-informed factors should be considered.

- technology novelty (e.g., first-of-a-kind digital instrumentation and control)
- system complexity (e.g., integrated systems with multiple interfaces)
- recent modifications (e.g., design changes, software updates, configuration changes).

In some cases, field changes may be implemented that do not go through the normal design change process. Inspectors should remain aware of the potential for such changes to impact cybersecurity.

Scalability:

Inspectors shall select a number of CDA samples for inspection based on the reactor plant design. Some reactor plants, such as stand-alone microreactors, are expected to have few CDAs compared to larger reactors. Typically, for a large reactor design such as AP1000, the inspection scope may include between 20 and 40 CDAs. For microreactors, the typical inspection scope may be 10 to 20 CDAs. Inspectors should coordinate with OAR/AROB to determine the scope of specific reactor design inspections.

Sample selection:

The permit holder or licensee is required by its CSP to perform a cybersecurity assessment and consequence analysis for each identified Critical System (CS), in accordance with NEI guidance (NEI 08-09, Sections A.3.1.1 through A.3.1.3) and NRC Regulatory Guide 5.71 (Sections C.3.1 through C.3.1.4). This analysis must identify the potential impact on SSEP functions if a CS is

compromised, exploited, or fails due to a cyberattack. Inspectors shall use this consequence information to inform system selection.

Inspectors shall review the version of NEI 13-10, "Cyber Security Control Assessments," adopted by the permit holder or licensee. This document provides industry guidance for applying cybersecurity controls. Inspectors must verify that the permit holder's version has been accepted by the NRC and shall familiarize themselves with the definitions of direct and indirect Critical Digital Assets (CDAs), including the control requirements applicable to each.

The inspector shall select three safety-related or security digital CSs associated with SSEP functions for inspection. These selections shall be based on the permit holder's or licensee's consequence assessments.

In addition, the inspector shall select:

- Security Architecture CDAs, due to their consistently high consequence in cybersecurity contexts.
- Additional CDAs selected using a risk-informed approach that ensures diversity of attack pathways (wired, connectivity, wireless connectivity, physical access, supply chain, and portable media and devices) are represented in the inspection. These CDAs must be associated with the three previously selected CSs.

Requirement 02.01, 02.04, 02.05, 02.06, and 02.07 are programmatic in nature and do not require CS or CDA samples. Inspectors shall select eight programmatic samples to evaluate the eight components of this requirement. Requirements 02.02 through 02.03 focus on implementation of cybersecurity controls. Inspectors should use the three selected CSs and CDAs to evaluate these requirements.

02.01 Attack Mitigation, Incident Response, and Contingency Planning

- a. **Verify that the permit holder has addressed security alerts and advisory notifications in accordance with the CSP. (NEI (E.3.5) RG (C.3.5))**

Specific Guidance

Site, corporate, and industry operating experience sources, along with alerts and advisories from the NVD database, the CISA database, and direct notifications from vendors (with whom the licensee has a contractual support relationship for vulnerability notifications). Select a sample of these sources and determine if the permit holder is meeting the requirements of their cybersecurity plan. The inspector(s) will select those controls that are highlighted with an asterisk* as part of the selected set of controls.

- b. **Verify that the permit holder has addressed attack mitigation, incident response and contingency planning policies and procedures in accordance with the CSP. (NEI (A.4.7, E.7, E.8) RG (C.3.3.2.7, C.8, C.9))**

Specific Guidance

Attachment 1 lists those controls related to attack mitigation, incident response and contingency planning. Select a sample of the listed controls and review how the permit holder addresses them, as well as the permit holder's effectiveness assessment.

(NEI (A.3.1.4, A.4.4.3.1) RG (A.3.1.4, A.3.1.6, A.4.1.2)) The inspector(s) should select those controls that are annotated with an asterisk* as part of the selected set of controls.

2.02 Program Monitoring, Assessment, Configuration, and Change Management

- a. **Verify that the permit holder addresses program monitoring, assessment, configuration, and change management controls in accordance with the CSP. (NEI (A.4.4, E.10) RG (A.4.1, C.11))**

Specific Guidance

Attachment 1 lists those controls related to program monitoring, assessment, configuration, and change management. Select a sample of the listed controls and review how the permit holder addresses them, as well as the permit holder's effectiveness assessment. (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)) The inspector(s) should select those controls that are highlighted with an asterisk* as part of the selected set of controls.

02.03 CDA and Information Protection

- a. **Verify that the permit holder addresses CDA and information protection controls in accordance with the CSP.**

Specific Guidance

Attachment 1 lists those controls related to digital CDA and information protection. Select a sample of the listed controls and review how the permit holder addresses them. (NEI (A.3.1.4, A.4.4.3.1) RG (A.3.1.4, A.3.1.6, A.4.1.2)) The inspector(s) should select controls that are annotated with an asterisk* as part of the selected set of controls.

02.04 Defense in Depth, Detection and Response

- a. **Verify the permit holder implemented and documented a defensive architecture in which the permit holder has established the required level of cybersecurity through the creation of a multi-level security architecture that provides for cybersecurity defensive levels separated by security boundary devices, such as firewalls, air gap, and/or deterministic devices, in which digital communications are monitored and restricted in accordance with requirements.**

Specific Guidance

Select a sample of the listed controls in attachment 1 of this IP and review how the permit holder or licensee addresses them as well as the permit holder's effectiveness assessment. (NEI (A.3.1.6, A.4.3, E.6), RG (C.3.4, C.7, A.3.1.5, A.3.1.6)) The inspector(s) should select those controls that are highlighted with an asterisk* as part of the selected set of controls.

- b. **Verify the permit holder has addressed, implemented, and documented malicious code protection mechanisms and such mechanisms have been deployed to detect and eradicate, mitigate the consequences of malicious code and that the permit holder has implemented monitoring capabilities of inbound and outbound communications and logging of unusual or unauthorized activities or conditions**

and provide real-time alerts when indications of compromise or potential compromise occur in accordance with regulatory requirements.

Specific Guidance

Select a sample of the listed controls from attachment 1 of this IP and review how the permit holder addresses them as well as the permit holder's or licensee's effectiveness assessment. (NEI (D.1.4, D.5.2, E.3.1, E.3.3, E.3.4, and E.6) RG (B.1.4, B.5.2, C.3.1, C.3.3, C.3.4, and C.7)) The inspector(s) should select those controls that are highlighted with an asterisk* as part of the selected set of controls.

- c. **Verify that the permit holder's implementation and documentation of communications monitoring ensure that staff are alerted and that the staff are trained in their alert response responsibilities in accordance with requirements. (NEI (E.3.1, E.3.4, E.6) RG (C.3.1, C.3.4, C.7))**

Specific Guidance

Attachment 1 lists those controls related to defense in depth and detection and response. The inspector(s) should select a sample of the listed controls and review how the permit holder addresses them as well as the permit holder's effectiveness assessment as applied to the digital CSs selected. (NEI (A.3.1.4, A.4.4.3.1) RG (A.3.1.6, A.4.1.2)) The inspector(s) should select those controls that are highlighted with an asterisk* as part of the selected set of controls.

02.05 Identification and Resolution of Problems

- a. **Verify that the permit holder is identifying issues related to the cybersecurity program at an appropriate threshold and entering them into the corrective action program. (NEI (A.2.2.11) RG (A.4.3)) Verify that the permit holder has appropriately resolved the issues regarding regulatory requirements for a selected sample of problems associated with the cybersecurity program. Refer to IP 88110, "Quality Assurance: Problem Identification, Resolution and Corrective Action (PIRCA) (Construction, Pre-Operation and Operation)," for additional guidance. (10 CFR 73.54(d) (2) and 10 CFR 73.55(b) (10))**

Specific Guidance

None.

02.06 Review Changes to the CSP

- a. **If the permit holder has made any changes to the CSP, verify the permit holder has performed an analysis to determine the changes have not decreased the effectiveness of the CSP, in accordance with regulatory requirements.**

Specific Guidance

Review 50.54(p), security impact analyses, and other applicant identified documentation supporting the CSP change, and determine if the CSP's effectiveness is equal to or increased beyond the original version.

- b. **If the permit holder has not made any changes to the CSP since the IP 75100.09 inspection, close this inspection item and consider it complete for the inspection requirements.**

Specific Guidance

None.

02.07 Cybersecurity Event Reporting

- a. **Review permit holder processes and procedures and verify the permit holder has met or is prepared to meet the cybersecurity event reporting requirements in accordance with regulatory requirements.**

Specific Guidance

Review documentation and implementation procedures, as well as perform personnel interviews to verify that responsible staff understand their role in reporting cybersecurity events.

75100.15-03 RESOURCE ESTIMATE

Approximately 120 hours of inspection effort are allocated for this IP. This estimate may vary depending on site-specific considerations.

75100.15-04 PROCEDURE COMPLETION

This IP is complete when sufficient inspection activities are performed to accomplish the IP objectives. Consult with the chief, Advanced Reactor Oversight Branch if needed to determine IP completion.

75100.15-05 REFERENCES

10 CFR 73.1 "Purpose and scope"

10 CFR 73.54 "Protection of digital computer and communication systems and networks"

10 CFR 73.55 "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage"

10 CFR 73.77 "Cyber security event notification"

IP 88110, "Quality Assurance: Problem Identification, Resolution and Corrective Action (PIRCA) (Construction, Pre-Operation and Operation)"

RG 5.71, "Cyber Security Programs for Nuclear Facilities"

NEI 08-09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors" ([ML101550069](#))

NEI 13-10, "Cyber Security Control Assessments"

END

List of Attachments

Attachment 1: Identification of Security Controls

Attachment 2: Revision History for 75100.15

Attachment 1: Identification of Security Controls

PURPOSE: This attachment is provided to identify the security controls that need to be considered in regard to the specific inspection activities of this IP.

BACKGROUND: The permit or license holder's CSP includes two appendices that list cybersecurity controls. Certain controls are associated with applicable inspection activities listed below. This does not preclude the inspector(s) from reviewing how other controls in the CSP are addressed by the licensee.

DISCUSSION: The following security controls are grouped and associated with specific areas of inspection effort. Those controls that are highlighted (with an asterisk*) are those that were previously deemed to be of most importance and are recommended for review.

The following are controls associated with section 02.02 attack mitigation, incident response and contingency planning:

Inspector(s) may observe a permit or license holder's exercise or tabletop to review how some of the controls listed below are addressed.

- a. Incident Response Policy and Procedures (NEI (E.7.1) (RG) (C.8.1))*
- b. Incident Response Training (NEI (E.7.2) RG (C.8.2))
- c. Incident Response Testing and Drills (NEI (E.7.3) RG (C.8.3))*
- d. Incident Handling (NEI (E.7.4 and A.4.6) RG (C.8.4 and C.13.3))*
- e. Incident Monitoring (NEI (E.7.5) RG (C.8.5))
- f. Incident Response Assistance (NEI (E.7.6) RG (C.8.7))
- g. Evaluating and Responding to Security Alerts and Advisories (NEI (E.3.5) RG (C.3.5))*
- h. Auditable Events, Records, and Time Stamps (NEI (D.2.2, D.2.8) RG (B.2.2, B2.8))
- i. Audit Generation (NEI (D.2.12) RG (B.2.7))
- j. Contingency Plan Testing (NEI (E.8.2) RG (C.9.3))*
- k. Recovery and Reconstitution (NEI (E.8.6) RG (C.9.7))

The following are controls associated with section 02.03 program monitoring, assessment, configuration, and change management:

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

The following are controls associated with section 02.04 CDA and Information protection:

- a. Security Function Isolation (The purpose of this control is to protect security applications from infections emanating from a co-mingled non security application.) (NEI (D.3.2) RG (B.3.2))
- b. Where Proprietary and Third Party Protocols are used which do not provide for detection of attack, alternative controls are implemented that provide for detection of attacks (NEI (D.1.20) RG (B.1.20))*
- c. Shared Resources (NEI (D.3.3) RG (B.3.3))
- d. Denial of Service Protection (The purpose of this control is to mitigate the effects of bandwidth or processing overloads which are the results of denial-of-service attacks.) (NEI (D.3.4) RG (B.3.4))
- e. Transmission Integrity, Confidentiality, and Session Authenticity (The purpose of this control is to detect, mitigate, and prevent “man-in-the-middle” attacks and to prevent unauthorized disclosure of information during transmission.) (NEI (D.3.6, D.3.7, and D.3.17) RG (B.3.6, B.3.7, and B.3.18))
- f. Cryptographic Key Establishment and Management (NEI (D.3.9) RG (B.3.9))
- g. Unauthorized Remote Activation of Services (NEI (D.3.10) RG (B.3.11))
- h. Transmission of Security Parameters (NEI (D.3.11) RG (B.3.12))
- i. Mobile Code (The purpose of this control is to mitigate malicious infection through mobile code.) (NEI (D.3.13) RG (B.3.14))
- j. Secure Name/Address Resolution (The purpose of this control is to ensure name/address resolution is authentic.) (NEI (D.3.14 and D.3.15) RG (B.3.15 and B.3.16))
- k. Public key certificates are issued under a certificate policy from an approved provider (NEI (D.3.12) RG (B.3.13))
- l. Confidentiality of Information at Rest (NEI (D.3.19) RG (B.3.20))
- m. User Identification and Authentication (NEI (D.4.2) RG (B.4.2))*
- n. Password Requirements (NEI (D.4.3) RG (B.4.3))
- o. Device Identification and Authentication (The purpose of this control is to prevent unknown, uncontrolled, and unauthorized portable electronic devices, storage media, and test equipment from being connected to and communicating or exchanging data with CDAs.) (NEI (D.4.5) RG (B.4.5))
- p. Authenticator Feedback (NEI (D.4.8) RG (B.4.8))
- q. Cryptographic Module Authentication (NEI (D.4.9) RG (B.4.9))

- r. Removal of Unnecessary Services, Programs, and Functionality (The purpose of these controls is to limit the amount of attack pathways and surface which an adversary can use to adversely impact a function.) (NEI (D.3.18, D.5.1) RG (B.3.19 and B.5.1))*
- s. Changes to File and Operating System Permissions (NEI (D.5.3) RG (B.5.3))
- t. Protocol Restrictions (The purpose of this control is to restrict the use of open/insecure communication protocols to protect CDAs from attacks that take advantage of the protocol's lack of security features.) (NEI (D.1.16) RG (B.1.16))

The following are controls associated with section 02.05 Defense in Depth, Detection and Response protection:

- a. Hardware Configuration (Note that communication ports can be both programming ports, serial, parallel, synchronous, and asynchronous.) (NEI (D.5.4) RG (B.5.4))
- b. Least Functionality (Of specific interest to the inspector(s) will be the use of white-lists and black-lists to control unwanted application execution.) (NEI (E.10.8) RG (C.11.8))*
- c. Resource Priority (NEI (D.3.5) RG (B.3.5))
- d. Host Intrusion Detection (NEI (D.5.2) RG (B.5.2))*
- e. System Integrity Policy and Procedure (NEI (E.3.1) RG (C.3.1))
- f. Malicious Code Protection (NEI (E.3.3) RG (C.3.3))*
- g. Monitoring Tools (NEI (E.3.4) RG (C.3.4))*
- h. Defense in Depth (NEI (E.6) RG (C.7))*
- i. Defensive Architecture Implementation (NEI (A.4.3) RG (C.3.2.1))*
- j. Software and Information Integrity (NEI (E.3.7) RG (C.3.7))
- k. Information Flow Enforcement. (NEI (D.1.4) RG (B.1.4))

Attachment 2 - Revision History for IP 75100.15

Commitment Tracking Number	Accession Number Issue Date Change Notice	Description of Change	Description of Training Required and Completion Date	Comment and Feedback Resolution Accession Number (Pre-Decisional, Non-Public)
N/A	ML26243A442 10/20/26 CN 26-048	Initial Issuance.	TBD	ML25072A126