
INSPECTION PROCEDURE 75100 ATTACHMENT 09

CYBERSECURITY DURING CONSTRUCTION OF ADVANCED REACTORS: PRE-FUEL ARRIVAL

Effective Date: 10/20/2026

PROGRAM APPLICABILITY: IMC 2203

STRATEGIC PERFORMANCE AREA: Security and Safeguards

75100.09-01 INSPECTION OBJECTIVES

- 01.01 To provide assurance that the cybersecurity program for a power reactor is properly being established in accordance with the regulatory requirements and the NRC approved cybersecurity plan (CSP) prior to site acceptance of reactor fuel.
- 01.02 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 regulatory requirements and the NRC approved CSP.

75100.09-02 INSPECTION REQUIREMENTS

General Guidance

This inspection procedure works in conjunction with the inspection procedure (IP) 75100.15, "Cybersecurity Inspection During Construction of Advanced Reactors: Pre-Operations," and verifies many aspects of the applicant's cybersecurity plan. This IP is scheduled after the applicant has started construction, has established their cybersecurity assessment team (CSAT) and cybersecurity plan, and before fuel arrives on site as required by Title 10 of the *Code of Federal Regulations* (10 CFR) 73.55(a)(4). 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.

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

Alternative controls may be implemented. Inspectors should 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 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, 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 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 holder's or licensee's CSP.

Risk-Informed Selection Considerations:

Boundary devices should always be inspected, when practical.

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 RG 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.

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 or licensee's version has been accepted by the NRC and shall familiarize themselves with the definitions of direct and indirect CDAs, including the control requirements applicable to each.

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, 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 should be associated with the three previously selected CSs.

Requirement 02.01 is programmatic in nature and does not require CS or CDA samples. Requirements 02.02 through 02.05 focus on implementation of cybersecurity controls. Inspectors should use the selected CSs and CDAs to evaluate these requirements.

02.01 Establish a Cybersecurity Program and Personnel Training

- a. **Verify a CSAT is being or has been established and the team is/has been performing its roles and responsibilities in accordance with the CSP. (NEI A3.1.2)(RG 5.71 3.1.2)**

Specific Guidance

Review documentation, implementing procedures, license conditions, perform personnel interviews, and observe applicable permit holder or licensee personnel performing their duties to ensure that the applicant has established its CSAT as described in the permit holder's or licensee's CSP.

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

Specific Guidance

Review the list of CSAT members along with their training and education background and determine if they meet the breadth of roles required.

- c. **Verify that the permit holder or licensee has established and implemented a cybersecurity program in accordance with its CSP. (NEI (A.4 through A.4.13) RG (C.2 through C.5))**

Specific Guidance

Review documentation, implementing procedures, perform personnel interviews to ensure that the applicant has established its cybersecurity program.

- d. **Verify that personnel and contractors are trained in accordance with the CSP. (NEI (E.9.1 through E.9.8) RG (C.10.1 through C.10.10))**

Specific Guidance

Areas inspector(s) should consider for review are how the cybersecurity program is being incorporated into and implemented with other programs to meet the cybersecurity program requirements.

02.02 Identification and Documentation of CSs and CDAs

- a. **Verify that the permit holder or licensee has identified all CSs and CDAs. (NEI 3.1.3, RG 3.1.3)**

Specific Guidance

Review documentation and implementing procedures, license conditions, as well as perform personnel interviews to verify all has identified the CSs and CDAs that must be protected in accordance with the permit holder's or licensee's CSP and regulatory requirements have been identified. A selected review of the identified CSs/CDAs and of a sample of digital computer and communication systems and networks that were not identified as being CSs/CDAs (excluded elements) is a good starting point for the inspector(s) to review implementation of this requirement.

Conduct a walk down of at least three CSs identified for this inspection. Refer to the permit holder's or licensee's definition of a CS and CDA in the CSP. The inspector(s) should also note that support systems and equipment that, if compromised, would adversely impact SSEP functions are also required to be protected in accordance with regulatory requirements. The inspector(s) should randomly select at least three CS/CDAs and review the documentation set consistent with the requirement. (NEI 3.1.3, RG 3.1.3)

02.03 Systems and Services Acquisition and Supply Chain Protection

- a. **Verify that the systems/services acquisition and supply chain protection controls have been/are being implemented in accordance with the CSP.**

Specific Guidance

Review procurement specifications, factory and site acceptance testing plans/results, in addition to appropriate references and documentation noted herein, to complete this inspection item. Attachment 1 lists those controls related to systems/services acquisition and supply chain protection. The inspector(s) will select between three and four of the listed controls and review how these controls are being addressed each as well as the effectiveness assessment for each. (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) will select those controls that are highlighted (with an asterisk*) as part of the selected set of controls. Permit holders or licensees may elect not to implement, implement an alternative, or implement the controls as specified. The permit holder or licensee may also implement manual/operator actions in place of the specified controls. Please see the general guidance in section 75100.09-02 of this IP.

02.04 Access Control and Media and Portable Device Protection

- a. **Verify attack vectors and access control restrictions associated with portable media and mobile have been/are being implemented in accordance with the CSP.**

Specific Guidance

Attachment 1 lists those controls related to access control and media and portable device protection. Select between eight and sixteen of the listed controls and review how the controls have been /are being implemented. (NEI (A.3.1.4, A.4.4.3.1, D.1.1 through D.1.23) RG (A.3.1.4, A.3.1.6, A.4.1.2, B.1.1 through B.1.23)) The inspector(s) will select those controls that are highlighted (with an asterisk*) as part of the selected set of controls. The controls may not be implemented, or alternative controls may be implemented, or the controls may be implemented as specified. Manual/operator actions may be implemented in place of the specified controls. Please see the general guidance in Section 75100.09-02 of this IP.

02.05 Implementation and Commencement of Ongoing Monitoring and Assessment Activities

- a. **Verify that the ongoing monitoring and assessment activities for those CSs or CDAs whose security controls have been implemented are being implemented in accordance with the CSP. (4.4)**

Specific Guidance

None.

75100.09-03 RESOURCE ESTIMATE

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

75100.09-04 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.

75100.09-05 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"

RG 5.71, "Cyber Security Programs for Nuclear Facilities"

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

NEI 08-09, Revision 6, Addendum 1, "Change Descriptions and Justifications" ([ML17079A379](#))

NEI 13-10, "Cyber Security Control Assessments" (Inspectors should review the version adopted by the permit holder or licensee and has been found acceptable for use by the NRC.)

END

List of Attachments

Attachment 1: Identification of Security Controls

Attachment 2: Revision History for 75100.09

Attachment 1: Identification of Security Controls

PURPOSE: This attachment is provided to identify the security controls that need to be considered while performing this inspection.

BACKGROUND: The permit or license holder's CSP includes two appendices that list cybersecurity controls. Certain controls are associated with applicable inspection activities. 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. The 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 02.03 systems/services acquisition and supply chain protection:

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

(Procurement specifications, factory and site acceptance testing plans/results, in addition to other services and acquisition documentation are good sources for how licensees address these requirements. Inspector(s) should notify the Quality Assurance and Vendor Branch (QAVB) in the Office of the Chief Nuclear Reactor Inspector (CNRI) of vendors/suppliers associated with systems or services acquisition in your inspection samples.)

The following are controls associated with section 02.04 access control and media and portable device protection:

- a. Access Control Policy and Procedures (NEI (D.1.1) RG (B.1.1))
- b. Account Management (The purpose of this control is to ensure that unauthorized accounts are eliminated. Inspectors should consider support from contractors when inspecting this line item.) (NEI (D.1.2) RG (B.1.2))
- c. Access Enforcement (NEI (D.1.3) RG (B.1.3))
- d. Separation of Functions and Least Privilege (The purpose of this control is to separate function authority between users and minimize user privileges so no one user can independently conduct malicious actions. Inspectors should consider support from contractors when inspecting this line item.) (NEI (D.1.5 and D.1.6) RG (B.1.5 and B.1.6))

- e. Unsuccessful Login Attempts (NEI (D.1.7) RG (B.1.7))
- f. Previous Logon Notification (NEI (D.1.9) RG (B.1.9))
- g. Access Control Supervision and Review (The purpose of this control is to prevent, or at least timely detect unauthorized access to, or unapproved manipulation of CSs and CDAs.) (NEI (D.1.11) RG (B.1.11))*
- h. Access Control for Portable and Mobile Devices (Inspectors should consider support from contractors when inspecting this line item.) (NEI (D.1.19) RG (B.1.19))*
- i. Wireless Access Restrictions (NEI (D.1.17) RG (B.1.17))*
- j. Network Access Control (NEI (D.1.15) RG (B.1.15))
- k. Public Access Protections (NEI (D.1.23) RG (B.1.23))
- l. Audit and Accountability Policy and Procedures (NEI (D.2.1, D.2.2) RG (B.2.1, B.2.2))
- m. Audit Review, Analysis, and Reporting (Inspectors should consider support from contractors when inspecting this line item.) (NEI (D.2.6) RG (B.2.6))
- n. Identification and Authentication Policies and Procedures (NEI (D.4.1) RG (B.4.1))
- o. Non-authenticated HMI Security (NEI (D.4.4) RG (B.4.4))
- p. Identifier Management (NEI (D.4.6) RG (B.4.6))
- q. Authenticator Management (NEI (D.4.7) RG (B.4.7))
- r. Media Protection Policy and Procedures (NEI (E.1.1) RG (C.1.1))
- s. Media Access (NEI (E.1.2) RG (C.1.2))
- t. Media sanitization whereby digital media are sanitized prior to disposal or release for reuse to eliminate transport of malicious software (malware) via portable media. (Inspectors should consider support from contractors when inspecting this line item.) (NEI (E.1.6) RG (C.1.6))*
- u. Personnel Security Policy and Procedures (NEI (E.2.1) RG (C.2.1))
- v. Personnel Termination/Transfer (NEI (E.2.2) RG (C.2.2))
- w. Controlling Maintenance Tools (NEI (E.4.2) RG (C.4.2))*
- x. Physical and Operational Environmental Protection Policy and Procedures (NEI (E.5.1) RG (C.5.1))
- y. Physical Access Authorization (NEI (E.5.4) RG (C.5.4))
- z. Physical Access Control (NEI (E.5.5) RG (C.5.5))*

- aa. Management of Personnel Performing Maintenance and Testing Activities. (NEI (E.4.3) RG (C.4.3)) *

The following are controls associated with section 02.05 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))*

Attachment 2: Revision History for IP 75100.09

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	ML26243A445 10/20/26 CN 26-048	Initial IP issuance to support IMC 2203.	TBD	ML25071A343