INSPECTION PROCEDURE 71130 ATTACHMENT 10

CYBERSECURITY

Effective Date: January 1, 2026

APPLICABILITY: IMC 2201 A

CORNERSTONE: Security

INSPECTION BASES: See IMC 0308 Attachment 6

This inspection procedure includes requirements that apply to all inspections (Sections 03.01-03.04) and requirements that apply only to inspections that review performance metrics and/or performance testing (Section 03.05). The use of performance metrics is voluntary and does not impact the overall inspection hours. Because licensees who have a performance testing program can demonstrate effectiveness of their cybersecurity programs in a performance-based manner, the oversight structure for these licensees differs from that of licensees without performance testing programs. The differences are described below.

SAMPLE REQUIREMENTS:

Sample Requirements		Minimum Baseline Completion Sample Requirements		Budgeted Range	
Sample Type	Section	Frequency	Sample Size	Samples	Hours
Cybersecurity Without Performance Testing	03.01 – 03.04 See Note 2, 03.05.b (as applicable)	Triennial	3	3	70 +/- 7
Cybersecurity With Performance Testing (Note 1 below)	03.01 – 03.05.a See Note 2, (03.05.b, as applicable)	Triennial	3	3	45+/- 5

The estimated time to complete the inspection procedure's direct inspection effort is 70 hours (with a range of 63 to 77 hours) per site and will consist of 1 week of direct inspection effort on site with contractor support. This inspection is planned to be conducted as a team inspection. The team should consist of two regional inspectors and one subject matter expert (SME).

The sample size of three equates to inspectors choosing three critical systems (CSs). The inspection team will perform a review of previous inspection violations and consult with resident inspectors to ascertain current licensee performance to inform the inspection requirements. The

final approval of the inspection requirements will be based on Branch Chief approval or other direction by management.

The frequency at which this inspection activity is to be conducted is 1 week triennially (once every 3 years). The 1 week of the inspection will be conducted on site, contingent on licensee performance testing and performance metrics.

Note 1: Alternate Inspection Program for Licensees with Performance and Function Testing Program

When a licensee elects to demonstrate an authentic and realistic performance and function test of the cybersecurity network configuration, the opportunity could provide the inspection team with a more efficient method to evaluate the licensee's defensive architecture and selected program elements. If, based on onsite oversight of the performance testing configuration and implementation, the inspection team concludes that the licensee conducted an effective, acceptable performance and function test, then the subsequent conduct of the inspection is modified. For licensees with a performance and functional testing program, up to 15 hours of direct inspection effort is planned for performance and function test observation applicable to the site. Inspection of the performance and functional testing demonstration and reported results may satisfy certain inspection areas (i.e., performance testing results may satisfy inspection requirements: 03.01.a, 03.01.b, 03.02.a, and the performance testing demonstration may satisfy portions of 03.02.b, 03.02.d, and 03.03.a, as determined by the type and scope of the testing).

Note 2: Section 03.04, Review of Cybersecurity Program is not required for minimum sample completion but may be used by the team after consultation with the responsible Branch Chief.

This inspection is planned to be conducted as a team inspection. The team may consist of two inspectors, and one subject matter expert (SME).

71130.10-01 INSPECTION OBJECTIVE

01.01 To provide assurance that 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 CSP changes and reports are in accordance with 10 CFR 50.54(p). See Note 2 above.

71130.10-02 GENERAL GUIDANCE

02.01 Background

Evaluation of the CSP implementation occurred in three distinct phases prior to development of this cybersecurity baseline inspection. Initial inspections in accordance with Temporary Instruction 2201/004, "Inspection of Implementation of Interim Cybersecurity Milestones 1-7," verified licensees established a qualified cybersecurity assessment team, identified all critical systems (CSs), and critical digital assets (CDAs), effectively implemented a network architecture to separate higher cybersecurity levels from lower levels as described in their CSP,

established controls for portable media, and mobile devices (PMMD), expanded their insider mitigation program to include personnel associated with cybersecurity assets, and implemented controls for CDAs to the most important systems.

The second phase of inspections verified that licensees implemented effective corrective actions for performance deficiencies identified during the Milestones 1 to 7 inspections.

The final phase of inspections, starting in 2017, verified licensees had fully implemented their cybersecurity programs. The full implementation inspections (a.k.a., "Milestone 8 inspections") were conducted using Inspection Procedure (IP) 71130.10P, "Cyber Security." 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 6, 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

The inspection process should focus on evaluating changes to the cybersecurity program, CSs, and CDAs. 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, SSEP functions. On a sampling basis, inspection team should be sensitive to CSs, digital assets, and CDAs that utilize software to accomplish SSEP and/or design functions. If the licensee has not completed any design changes since the last inspection, the team may consider reviewing information on potential software vulnerabilities by utilizing tools such as the National Vulnerability Database (NVD) to identify any potential vulnerabilities for sampling selection of equipment to inspect. If no changes have occurred through the design change process or identified via operating experience sources, then the inspection team should select at least three systems, including one safety-related or important-to-safety system, and one security system, for review of program lifecycle management. The selection of the safety-related CS should utilize established risk-informed data, while the security CS should emphasize a security function using the consequence-based methodology. If SSCs are selected outside these criteria, the selection should emphasize implications for plant transients. Inspectors should leverage the insights of the resident inspector staff, and regional Senior Reactor Analyst (SRA) during the sample selection process. Inspectors are highly encouraged to utilize internal databases maintained by the Operating Experience Branch in the Division of Reactor Oversight such as the Generic Communication/Inspection Procedure crosswalk for sample selection or utilize the nonpublic Standardized Plant Analysis Risk (SPAR) dashboard.

When preparing, planning, and conducting this inspection, the inspector(s) may need additional guidance in implementation requirements. The inspector(s) should review Security Frequently Asked Questions (SFAQs) related to cybersecurity requirements in advance of inspections. If the inspector requires policy interpretation or program clarification, then they should consult with the Cybersecurity Branch liaison assigned to the inspection for immediate resolution. All findings and issues related to this IP shall be reviewed using the SIF process.

71130.10-03 INSPECTION REQUIREMENTS

Verify that digital computer and communication systems and networks associated with SSEP functions are adequately protected against cyberattack. Verify that the licensee is maintaining a cybersecurity program in accordance with its CSP and 10 CFR 73.54. The inspector will consider the following inspection requirements when developing the inspection plan and identifying the inspection sample.

Note for Completion: Sections 03.01 to 03.04 constitute the areas in this procedure that include the inspection requirements.

(Section 03.04 is not required for minimum sample completion.) In accordance with NRC ADVANCE Act initiatives, IMC 2515, "Light-Water Reactor Inspection Program – Operations Phase," has been revised to direct NRC inspections be completed at the minimum level necessary. Specifically, the IMC was revised to state:

> "Inspectors should inspect to the minimum number of samples specified by the baseline inspection procedure. The specified minimum sample provides the insights necessary to assess performance, with performance indicators, in each cornerstone of safety. Items for consideration to conduct the above minimum sample are: 1) risk significance of the SSC or evolution, 2) current performance of the licensee, 3) the work the sample will be replacing, and 4) the site has reactors with different technologies (i.e. unique site budget model sites). If the inspectors believe there will be no value added in the assessment of the licensee in conducting samples above minimum, then the inspector should complete Inspection Procedures at minimum samples."

As part of the inspection, inspectors may review a sample of licensee corrective actions to determine whether the issues were appropriately identified, documented, evaluated, and corrected in accordance with the licensee's corrective action program. If a licensee develops performance testing or performance metrics as described in Section 03.05, and found satisfactory through review by the inspection team, then identified sections should be evaluated as complete, and the inspection should focus on the remaining areas not demonstrated by the performance testing or metrics, as described in this IP. Section 03.05 and the associated documents mentioned below shall describe the standards for determining satisfactory demonstration. The attributes of completion of inspection requirements will be based on the review of the licensee performance and smart-sampling process using a risk-informed consequence-based approach. The inspectors can also utilize data from the Plant Risk Information Book (PRIB) to support sample selection. The PRIB provides a summary of PRA results from the SPAR model in terms of contribution to the core damage frequency (CDF). When using the risk-informed and consequence-based approach to complete cybersecurity inspections, inspectors should consider these criteria. Inspectors will select a total of 3 CSs (one system from each area) from safety, important to safety, 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, important to safety, security, and emergency

preparedness. While the safety and important to safety aspects can be quantified by various risk attributes, the security and emergency preparedness SSCs are elements that warrant a different measure of assessment. For safety and important to safety, inspectors should consider using the Birnbaum value to screen risk of an effected component. Birnbaum measures the rate of change in total risk as a result of changes to the probability of an individual basic event. The Birnbaum value is a rough estimate of the annualized delta CDF assuming an SSC is failed. A Birnbaum value of greater than 1E-6 should be considered risk significant. Using this metric, the SRA and the inspectors can quickly identify risk-significant SSCs and human actions. Inspectors should leverage the SRA to support this decision-making on using risk.

Risk-Informed Selection considerations:

Using the following consequence-based prioritization, inspectors should apply risk-informed considerations to refine the sample set. If available for the reactor's design, inspectors should review the PRA criteria referenced above to inform selection of the samples. 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. SEIM, IDS, IPS, Scanning/Data Transfer stations))
- Important-to-Safety (ITS) CDAs
- Balance of Plant (BoP) CDAs

This list above is not all inclusive of devices that should always be inspected. Inspectors should be sensitive to the licensee specific CSP attributes.

Safety considerations:

Does the CDA impact the integrity of the reactor coolant pressure boundary?

Does the CDA affect the capability to shutdown the reactor or maintain a safe-shutdown condition?

Does the CDA have implications for preventing or mitigating consequences of accidents as defined in 10 CFR 50.34(a)(1), 10 CFR 50.67(b)(2), or 10 CFR 100.11 or the CSP?

Does the CDA support the operability of the SSC?

Does the CDA prevent or adversely impact the performance of a Safety related function through direct interaction or through other means?

Does the CDA perform functions related to requirements for reduction of risk from anticipated transients without scram (ATWS), 10 CFR 50.62

Does the CDA impact functions required to support a loss of all alternating current (SBO) event, 10 CFR 50.63.

Does the CDA perform a function that has RG 1.97 implications?

Does the CDA perform a balance of plant function that could result in an unplanned reactor shutdown or transient?

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. In these cases, the loss of the device usually requires some level of compensatory measures to be established until corrected. Inspectors can ascertain specific functions by reviewing the attributes specified in NEI 10-04.

With most security functions, the loss of a security function leads to the establishment of compensatory measures until the deficiency is corrected, or the function can be restored. Inspectors should determine the compensatory measures established if the security function is lost to support sample selection.

- Security CDAs
- Network Security Architecture
- Emergency Preparedness (EP) CDAs
- Non-Critical Digital Assets (DAs)

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

- System Complexity (e.g., integrated systems with multiple interfaces),

Sample selection may:

- Exclude low-consequence CDAs per the NEI 13-10 definition (BoP and DAs)
- Limit moderate-consequence CDAs (EP and ITS) to no more than 10%

Security consideration:

- Does the CDA affect physical barriers?
- Does the CDA affect access controls?
- Does the CDA affect detection and assessment systems?
- Does the CDA affect a response requirement function?
- Does the CDA affect a Site Security Plan requirement?

Emergency Preparedness:

- Does the CDA have requirements identified in the Emergency Plan that can NOT be performed by diverse and independent means?

Additional guidance attributes can be reviewed in part, in NEI 10-04, Section 1.2.

Note: The paragraph references provided within parentheses for applicable sections below are based on NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," and Regulatory Guide (RG) 5.71, "Cybersecurity Programs for Nuclear Facilities." Both documents were determined by the NRC to be acceptable templates 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. Verify that the licensee conducts assessments required by the CSP. The basis for completing the inspection requirement is defined in the specific guidance section.

Specific Guidance:

The inspection of this control should be evaluated as complete, based on the successful conduct of the licensee's performance testing.

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. The licensee performs security assessments to verify security-related activities and actions occur at the frequency specified in security controls requirements or within the evaluated alternate control frequency. Inspectors should ensure ongoing monitoring of cybersecurity controls used to support CDAs are implemented consistently with the licensee's CSP. The NRC expectations for these objectives are identified, in part, in RG 5.71, Section 4.1, "Continuous Monitoring and Assessment," and A.4.1, "Continuous Monitoring and Assessment." (10 CFR 73.54(d)(2)).

b. Verify that the licensee conducts an appropriate effectiveness analysis as specified in the CSP. The basis for completing the inspection requirement is defined in the specific guidance section.

Specific Guidance:

The review requires an evaluation of the cybersecurity program and the required controls, at least every 24 months or at the frequency specified in the CSP. The inspection of this control should be evaluated as complete, based on the successful conduct of the licensee's performance testing.

The effectiveness analysis (i.e., NEI 08-09, Section 4.4.3.1, "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 may include, but are not limited to, periodic audits of the physical security program, security plans, implementing procedures, cybersecurity programs; safety/security interface activities; the testing, maintenance, and calibration program as it relates to cybersecurity; and feedback from the NRC and local, state and federal law enforcement authorities. The NRC expectations for these objectives are specified in part in RG 5.71, Sections A.4.1.2 and A.4.1.3.

c. Verify that the licensee performs vulnerability assessments or scans as described by the CSP, including the capability to correct exploited weaknesses. The basis for completing the inspection requirement is defined in the specific guidance section.

Specific Guidance:

The inspection of this control should be evaluated as complete, based on the successful conduct of the licensee's performance testing.

The vulnerability assessment program establishes programs/procedures for screening, evaluating, and dispositioning threat notifications, and vulnerabilities against CDAs received from a credible source. The licensee will use their corrective action program (CAP) to document the potential vulnerability and to initiate corrective actions. CAP evaluations should consider the threat vectors associated with the vulnerability.

Vulnerabilities that pose a risk to SSEP functions are mitigated or evaluated when the licensee implements remediation as required to maintain adequate defense-in-depth protective strategies. Dispositioning includes implementation, as necessary, of cybersecurity controls to mitigate newly reported or discovered vulnerabilities, and cyber threats. The NRC expectations for these objectives are specified in part in RG 5.7, Section A.4.1.3, "Vulnerability Assessments and Scans."

03.02 Defense-in-Depth Protective Strategies

a. Verify that the licensee maintained the defensive architecture, its capability to detect, to respond to, and to recover from cyberattacks, as described by the CSP. The basis for completing the inspection requirement is defined in the specific guidance section.

Specific Guidance

The inspection of this control should be evaluated as complete, based on the successful conduct of the licensee's performance testing.

Defense-in-depth protective strategies have been implemented, documented, and are maintained to ensure the capability to detect, delay, respond to, and recover from cyberattacks on CDAs. The CSP establishes controls to ensure that the licensee can detect, delay, respond to, and recover from cyberattacks. The controls may differ for the different cybersecurity defensive levels. Licensees may have implemented near real-time automatic detection mechanisms to capture logs and to generate alarms, 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).

Provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure effectiveness of the program. The NRC expectations for these objectives are specified, in part, in RG 5.71, Section A.3.1.5, "Defense-in-Depth Protective Strategies." (10 CFR 73.54(c)(2) and 10 CFR 73.55(b)(3)(ii)).

b. Verify that the licensee maintains controls and elements to ensure boundary protection for the cybersecurity levels and ensures that integrity of data is maintained. The basis for completing the inspection requirement is defined in the specific guidance section.

Specific Guidance:

These protections can include host intrusion protection for devices and network intrusion detection/prevention for their network flows. Portions of the inspection of this control should be evaluated as complete, based on the successful conduct of the licensee's performance testing.

To meet this requirement, inspectors will determine if licensees have maintained 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 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. This means that the most critical and sensitive systems, which need the highest level of security, are placed within multiple layers of protection. These layers, or boundaries, are designed to prevent unauthorized access.

Inspectors will determine if the defensive architecture has been implemented, documented, and is maintained to protect CDAs that have similar cyber risks from other CDAs, systems, or equipment by verifying logical, and physical boundaries used to control the data transfer between boundaries and between devices. The inspection team should review NEI 08-09, Section 4.3 and the applicable CSP sections to verify the actual implementation attributes.

Inspectors should verify that the licensee has analyzed digital computers and communications systems and networks and identified those assets that must be protected against cyberattacks to preserve the intended function of plant systems, structures, and components within the scope of the cybersecurity rule and accounted for these conditions in the design of the program. The inspection team can utilize the guidelines in NEI 08-09, Appendix E, Section 6, which provides attributes for the licensee to document and implement specific defensive strategy measures.

c. Verify that the licensee maintained the implemented security controls to provide high assurance that the CDAs are continuously protected against cyberattacks. The basis for completing the inspection requirement is defined in the specific guidance section.

Specific Guidance

Inspectors will ensure that the licensee is verifying and validating that the security controls are implemented correctly, operating as intended, and consistent with the cybersecurity controls credited in the licensee's CSP.

d. Verify that the licensee has established access controls and authentication and user- identification capabilities. The basis for completing the inspection requirement is defined in the specific guidance section.

Specific Guidance

Portions of the inspection of this control should be evaluated as complete, based on the successful conduct of the licensee's performance testing.

The inspectors should verify the licensee has established policies and procedures as required by the CSP (e.g., NEI 08-09, Appendix D, Section 1, "Access Control," and Section 4, "Identification and Authentication," or RG 5.71, Appendix B.4, "Identification and Authentication"). The licensee should also have policies and procedures for the periodic review of the access authorization list. The inspection team can also 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 team should also consider the applicability of 10 CFR 73.56 when verifying if individuals are trustworthy and reliable to implement the respective CSP. The NRC defined expectations for meeting this control are specified in RG 5.71, Appendix B.4, "Identification and Authentication."

e. Verify that the licensee has continued to control PMMD in accordance with their CSP. The basis for completing the inspection requirement is defined in the specific guidance section.

Specific Guidance

Licensees utilize PMMD to update software and manage changes to CDAs. Inspectors should verify that the licensee has established policies and procedures that describe the control, update, and use of PMMD, and that the CDA that is being maintained is hardened in accordance with the requirements of the CSP. The inspection team should be sensitive to the attack pathway created by using PMMD. Specifically, inspectors should verify that access to the CDA media is documented, controlled, and restricted to authorized individuals consistent with NEI 08-09, Appendix E, Section 1, "Media Protection," as well as those instances in which PMMD is used in maintenance activities as specified in NEI 08-09, Appendix E, Section 4.2, "Maintenance Tools," since unanticipated changes to the CDA can occur due to the use of these devices. The NRC's expectations for these control requirements are specified, in part, in RG 5.71, Appendix B.1.19, "Access Control for Portable Media and Mobile Devices," RG 5.71, Appendix C.1.2, "Media Access," RG 5.71, Appendix C.3.3, "Malicious Code Protection," and RG 5.71, Appendix B.1.1, "Access Control Policy and Procedures." Inspectors may also want to review SFAQ 16-01, 16-03 and 16-05 to support Anti-Virus (AV) Scanning Kiosks or AV Kiosk management systems/networks.

03.03 Configuration Management and Change Control

a. Verify that the licensee evaluates modifications to CDAs prior to implementation to assure that digital computer and communications systems and networks are adequately protected against cyberattacks. The basis for completing the inspection requirement is defined in the specific guidance section.

Specific Guidance

Portions of the inspection of this control should be evaluated as complete, based on the successful conduct of the licensee's performance testing if inclusive of design changes.

The inspection team should verify that licensees are implementing this requirement consistent with the performance requirements specified in 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 against cyber-attacks, up to and including the DBT (10 CFR 73.54(a)(1) and 10 CFR 73.54(d)(3)). These evaluations are typically performed as part of the licensee's configuration management program with oversight from the CSAT. The licensee incorporates the control of modifications to CDAs to ensure that they continue to be protected against cyberattacks and meet the requirements of their CSP.

Changes to CDAs are controlled using design control or configuration management procedures so that additional cybersecurity risk is not introduced into the system. The inspectors should verify that the implemented controls meet the requirements in the CSP. Inspectors should consider reviewing the requirement for Flaw Remediation in NEI 08-09, Appendix E, Section 3.2 or RG 5.71 Appendix C.3.2, which states, in part, to perform vulnerability scans or assessments of the CDA to validate that the flaw has been eliminated before the CDA is put into production, thus assessing the Security Impact Analysis of Changes and Environments.

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. The basis for completing the inspection requirement is defined in the specific guidance section.

Specific Guidance:

Portions of the inspection of this control should be evaluated as complete, based on the successful conduct of the licensee's performance testing.

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 interdependence of other CDAs or support systems and incorporates the assessment into the cybersecurity impact analysis. Inspectors should specifically review: Flaw Remediation in NEI 08-09 E.3.2 or RG 5.71 Section C.3.2 "Perform vulnerability scans

or assessments of the CDA to validate that the flaw has been eliminated before the CDA is put into production." ((NEI A.4.4.2, E.10.5) RG (C.11.5))

c. Verify that the licensee has implemented appropriate supply chain and services acquisition controls for the replacement of CDAs and/or newly acquired CDAs as they are applied to respective CSs. The basis for completing the inspection requirement is defined in the specific guidance section.

Specific Guidance:

Since many replacements for CDAs will be purchased as commercial off-the-shelf, a review of supply chain and acquisition controls should be performed, and the replacement and/or new acquisition CDAs should be hardened. This review should factor in the classification of the CDA and the overall risk to the plant. Inspectors should ensure that security requirements are included in every RFP and contract. Inspectors should evaluate aspects of the lifecycle of control asserted for the procured CDA as it is developed, tested, assessed prior to shipment to the licensee, received, assessed by the licensee, and stored prior to final implementation at the facility. Inspectors should be sensitive to software development attributes, where known, and determine if source code is maintained by the licensee. Inspectors should review the RG 5.71, Section 3.3.3.1, “Systems and Service Acquisition,” section which specifies further criteria. (RG 5.71, Section C.12, 1, RG 1.152, NEI 08-09, Appendix E, Section 11, “System and Services Acquisition”)

03.04 Review of the Cybersecurity Program (This section is not required for minimum sample completion.)

a. Verify that any changes to the CSP did not reduce the safeguards effectiveness of the plan. (Changes to the CSP can be made according to the requirements of 10 CFR 50.54(p)). The basis for completing the inspection requirement is defined in the specific guidance section.

Specific Guidance

The licensee will have a change management procedure and licensing basis administrative controls for making changes to their CSP. Further, the CSP requires that the licensee develop implementing procedures. Review of the procedures can be conducted for controls such as password requirements, testing control procedures, hardening guidelines, control of portable media, and any common, or administrative control. Inspectors should be sensitive to the 10 CFR 73.58 Safety/Security interface requirement when changes are being assessed.

b. Verify that the licensee established an incident response process, including contingency plans, and procedures. Verify that the licensee properly evaluated and responded to cybersecurity incidents, including effectively implementing their reporting requirements. The basis for completing the inspection requirement is defined in the specific guidance section.

Specific Guidance:

Identification, detection, and response to cyberattacks are typically directed by site procedures that govern responses to plant events. 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. Ensure that testing of the incident response capability for CDAs has occurred at least every 12 months.

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.

If available, observe a licensee-conducted Cybersecurity Incident Response drill to ensure that site-defined tests or drills are used, so that staff are aware of their roles and responsibilities, and that results of the drill are evaluated and documented. If not available, seek to perform table-tops of anticipated response activities.

c. Verify that the CSAT is functioning consistent with the approved CSP licensing basis. The basis for completing the inspection requirement is defined in the specific guidance section.

Specific Guidance:

Inspectors will verify that the CSAT is broadly represented by staff consistent with the approved cybersecurity plant. In instances where decisions regarding control assessments or programmatic procedures being approved without a functioning CSAT, inspectors should question the validity of such actions. Inspectors should verify that appropriate facility personnel, including contractors, are aware of cybersecurity requirements, and receive the training necessary to perform their assigned duties, and responsibilities

d. Verify that the licensee has established training as described in the CSP. The basis for completing the inspection requirement is defined in the specific guidance section.

Specific Guidance:

Ensure the licensee's cyber training requirements for personnel and contractors to perform their assigned duties and responsibilities in implementing the requirements of their cyber program are established, implemented, and documented. The licensee should have a training curriculum to include general awareness, technical, specialized, and situational awareness training. (10 CFR 73.54(d)(1)).

03.05 Evaluation of Performance Testing or Performance Metrics

a. If the licensee elects to demonstrate performance and function test(s), verify that the performance, and function testing reflects the on-site cyber system physical configuration, and performance.

Specific Guidance

Performance testing is a key element of most information technology program assessment programs. A performance testing program would provide the licensee with an opportunity to demonstrate how the elements of their cybersecurity program work together to provide defense-in-depth. Performance testing provides a realistic alternate

method to inspect the cybersecurity program's protection of safety, security, and emergency preparedness functions against a cyberattack.

This section is optional, and is not part of the inspection requirements, unless the option is elected to be implemented by the licensee. If elected, the performance testing results may satisfy inspection requirements 03.01.a, 03.01.b, and 03.02.a. Additionally, the performance testing demonstration and information reported may satisfy portions of 03.02.b, 03.02.d, 03.03.a, and 03.03.b inspection requirements as determined by the type and scope of the testing. If the performance testing and licensee submitted performance testing results demonstrate successful implementation of these performance requirements, then the inspection of the demonstrated inspection requirements should be evaluated as complete. If the performance testing does not properly demonstrate the fidelity of the cyber controls, then additional onsite inspection should be performed to assess the controls.

If the answers to the following are both "yes", then the inspector may determine that the demonstration of the performance and function test is adequate.

1. In accordance with the CSP, licensees are required to collect data, to document results, and to evaluate the effectiveness of existing cybersecurity programs, and cybersecurity controls. Did the licensee submit information that describes and documents the results of its performance testing assessment program as part of the request for information (RFI) submission?

2. Was the cyberattack performance and functional test authentic and realistic? Specifically, the virtual network test configuration had to reasonably match the site-specific computer network configuration(s) and the cyberattack testing performed and realistically challenged the virtual network.

   The observed performance test will be conducted at least 120 days before the start of the onsite week of inspection. Records or reports of completed licensee performance tests during the cycle will be provided to the inspection team in sufficient time prior to the NRC observed performance test. The lead time provides the NRC an opportunity to review the test plan and observe the test conduct. Test observation will facilitate the inspector's verification of the authenticity, realism, and integrity of the performance, and function test(s) and the decision of whether the testing and results provide enough information to reduce the on-site inspection scope.

   If multiple facilities want to credit a single testing facility, the licensee shall adequately demonstrate that the tested configuration accurately represents the network configurations and defensive architectures at the respective sites.

3. If the licensee identified issues during the performance testing, did they appropriately categorize and correct the deficiencies? If the testing deficiency revealed noncompliance with the CSP, did the licensee implement appropriate compensatory measures, prioritize the deficiency, and implement corrective actions? Licensees are required to monitor the cybersecurity program through random testing of cybersecurity intrusion monitoring tools, periodic functional testing, and vulnerability scans/assessments. Therefore, the results of licensee performance testing and areas requiring corrective action are part of normal licensee-required self-monitoring

activities and shall not be documented in the inspection report, in accordance with NRC Enforcement Policy. [A4.4.3.2, E3.4]

b. Performance Metrics

This section is optional, and is not part of the inspection requirements, unless the option is elected to be implemented by the licensee. If elected, the metric information provided by the licensee, along with any data needed to validate the reported metric result, during the RFI submission shall assist the inspection team to conduct a more efficient inspection effort and better inform the inspection team of the performance of the cybersecurity program. In accordance with the CSP, licensees are required to confirm information, document results, and evaluate the effectiveness of existing cybersecurity programs and cybersecurity controls. [A3.1.2].

Specific Guidance:

If the following metric data is provided to the inspection team during the RFI submission, the inspection team will review the submitted information during inspection preparation to evaluate the quality of the submitted information and gain insights into licensee performance in these inspectable areas. The RFI submission shall be submitted by licensees following the guidance in the performance metrics RFI Template which is part of the RFI package.

1. Access control

- Number of violations of access control policy identified during the sample period (the objective of the access control policy is to provide high assurance that only authorized individuals or processes acting on their behalf can access CDAs and perform authorized activities). [D1.1, D1.4, D1.11, and D2.6]. This value is used to evaluate the effectiveness of the access control policy and associated controls [D.1.1. D1.4, D1.11, and D2.6].

- Number of instances in which the time to disable and to remove user credentials of employees due to a change of duty or of employment went beyond the allotted time permitted in the CSP (reviews CDA accounts consistent with the access control list provided in the design control package, access control program, and cybersecurity procedures, and initiates required actions on CDA accounts in accordance with the CSP). [D1.2]. This value is used to determine whether the licensee is meeting the requirements of account management activities.

- Number of non-compliance incidents of cybersecurity controls by third-party personnel. [D1.1, D1.3, D4.5, and E5.2]. This metric is used to evaluate the licensee's capability to screen and to enforce security controls for third-party personnel.

- Number of unauthorized PMMD connected to CDAs [D1.18, D1.19]. This requirement involves monitoring, controlling, and documenting usage restrictions. This may be performed manually or digitally. Device identification and authentication at the CDAs [D4.5] could be used to provide input to this metric.

2. Flaw Remediation

   - Number of security flaws not mitigated (identify the security alerts and vulnerability assessment process, communicate vulnerability information, correct security flaws in CDAs, and perform vulnerability scans, or assessments of the CDA to validate that the flaw has been eliminated before the CDA is put into production). [E3.2 and E12]. This value informs the effectiveness of the technical evaluation and testing of recommended flaw remediation.

3. Periodic Review of Auditable Events

   - Number of configuration changes that are not documented or approved in accordance with the CSP or procedures, and the number of incorrect baseline configurations noted by the licensee through various methods, to include integrity verification (baseline configuration documentation includes the following: a list of components, for example, hardware and software, interface characteristics, security requirements, and the nature of the information communicated, configuration of peripherals, version releases of current software, and switch settings of machine components). This metric assists in describing the licensee's ability to manage configuration changes and to monitor systems for unauthorized changes. [E3.7, E10.3, and E10.4].

4. Malicious Code Identification

   - Number of incidents where malicious code was not detected at the security boundary device entry and exit points and on the network (real-time malicious code protection mechanisms are established, deployed, and documented for security boundary device entry, and exit points, CDAs (if applicable), workstations, servers, and mobile computing devices (i.e., calibrators) on the network to detect and eradicate malicious code resulting from data communication between systems, CDAs, removable media or other common means; and exploitation of CDAs vulnerabilities). Number of incidents where malicious code was not blocked from making unauthorized connections (monitoring events on CDAs, detecting attacks on CDAs, detecting, and blocking unauthorized connections, identifying unauthorized use of CDAs). [E3.3 and E3.4]. This value assists in the assessment of the effectiveness of malicious code protection controls and processes, as well as monitoring tools, and techniques.

   - Number of periodic scans not performed in accordance with procedures and periodicity requirements (perform periodic scans of security boundary devices, CDAs (if applicable), workstations, servers, and mobile computing devices at an interval commensurate with the associated risk determination, and real-time scans of files from external sources as the files are downloaded, opened, or executed, and disinfect, and quarantine infected files). [E3.3] This metric establishes whether licensees are correctly following procedures and performing periodic validation of boundary device tasks.

5. Security Functionality

   - Number of security functions not tested manually or through automated means (the correct operation of security functions of CDAs are verified and documented periodically, in accordance with 10 CFR 73.55(m), upon startup, and restart, upon command by a user with appropriate privilege, and when anomalies are discovered, when possible.) [E3.4, E3.6].

6. Security Awareness and Assessment Team

   - Personnel training and specialized training commensurate with their assigned duties are completed. [A4.8, E9.2, E9.3, and E9.4].

   - The minimum required staff was assigned, and any vacancies were filled with fully qualified, and trained personnel. [A3.1.2]

7. System Hardening

   - Number of CDAs with ports or protocols that had not been evaluated as physically and logically secured and hardened, including firewalls and boundary control devices that were removed. [E6]

71130.10-04 REFERENCES

10 CFR 73.54, “Protection of Digital Computer and Communication Systems and Networks”10 CFR 73.77, “Cybersecurity Event Notifications”

CYBERSECURITY: Guidance Document for Development of the Request for Information (RFI) and Notification Letter for Full Implementation of the Cybersecurity Inspection (ML17156A215)

Licensees’ 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)

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

Power Point Presentation describing the inspection and development history of cybersecurity (ML20324A636)

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)

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)

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)

RG 5.71, "Cybersecurity Programs for Nuclear Facilities" (ML090340159) (Package ML090340152)

RG 5.83, "Cybersecurity Event Notifications" (ML14269A388) (Package ML15188A548)

SFAQ. The SFAQ are considered "For Official Use Only – Security-Related Information" and are available, upon request, to stakeholders with appropriate need to know.

SFAQ	Title	Accession #
10-05	IT Functions for the Critical Group	ML102100070
10-06	Classification of Cyber Security Information	ML102090633
12-17	Cybersecurity Milestone 1	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	Unauthorized Person	ML16088A242
16-01	Data Integrity	ML16196A302
16-02	Deterministic Devices	ML16208A222
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

END

Attachment 1: Revision History for IP 71130.15

Attachment 1: Revision History for 71130.10

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	ML16350A051 05/15/17 CN 17-010	First issuance. This is a pilot program one-time inspection until December 31, 2020. This shall be converted to a baseline inspection in 2021. Completed 4-year search for commitments and found none.	None	ML16350A050
N/A	ML21155A209 09/03/21 CN 21-029	IP 71130.10 is being issued to include updates resulting from inspection feedback and revised to support realignment of agency document standards.	None	ML21155A207
N/A	ML21271A106 12/14/21 CN 21-040	IP 71130.10 is being re-issued to include updates to the description and background for the performance testing option.	None	Not Applicable
N/A	ML25337A110 03/24/26 CN 26-009	IP 71130.10 is being re-issued to support guidance updates based on NRC, NEI, and Public Comments.	None	ML25337A104