NRC INSPECTION MANUAL

NSIR/DPCP

INSPECTION PROCEDURE 71130 ATTACHMENT 10

CYBERSECURITY

Effective Date: January 1, 2022

PROGRAM APPLICABILITY: IMC 2201 Appendix A

CORNERSTONE: Security

INSPECTION BASES: See IMC 0308 Attachment 6, “Basis Document for Security Cornerstone of the Reactor Oversight Process”

This inspection procedure includes requirements that apply to all inspections (Sections 03.01-03.05) and requirements that apply only to inspections that review performance metrics and/or performance testing (Section 03.06). 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 testing programs. The differences are described below.

SAMPLE REQUIREMENTS:

Sample Requirements		Minimum Baseline Sample Completion Requirements		Budgeted Range	
Sample Type	Section(s)	Frequency	Sample Size	Samples	Hours
CyberSecurity Without Performance Testing	03.01 – 03.05, 03.06b (as applicable)	Biennial	1 per site	1	70 +/- 7
CyberSecurity With Performance Testing (Note 1 below)	03.01 – 03.06.a, (03.06b, as applicable)	Biennial	1 per site	1	42 +/- 5

The estimated time to complete the inspection procedure direct inspection effort is 70 hours (with a range of 63 to 77 hours) per site and will consist of one week of direct inspection effort with contractor support. This inspection is planned to be conducted as a team inspection. The team shall consist of two regional inspectors and two contractors.

The inspection of the minimum number of inspection requirements will constitute completion of one sample and this procedure. This inspection requirement range for completion is as follows: minimum of three inspection requirements, nominal four inspection requirements, and maximum, based on unusual circumstance, or special considerations, five inspection requirements. The inspection of the nominal range of inspection requirements within this procedure is the target range for this sample and should be completed to the extent practicable.

The frequency at which this inspection activity is to be conducted, is one week biennially (once every 2 years).

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 inspectors a more efficient method to evaluate the licensee's defensive architecture and selected program elements. If, based on on-site oversight of the performance testing configuration and implementation, the inspectors conclude 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 7 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, 03-01b, 03.02.a, and 03.02.e, and the performance testing demonstration may satisfy portions of 03.02.b, 03.02.d, 03.03a, and 03.03.b, as determined by the type and scope of the testing). As a result, the estimated time to complete the inspection procedure direct inspection effort shall be up to 42 hours per site, (35 hours for on-site inspection plus up to 7 hours for performance and function test observation, for an overall range of 37 to 47 hours per site). This inspection is planned to be conducted as a team inspection. The team may consist of one inspector, and two contractors for one week.

71130.10-01 INSPECTION OBJECTIVES

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 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).

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 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, 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 were conducted using Inspection Procedure (IP) 71130.10P, "Cybersecurity." 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) 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 program, critical systems, and CDAs. These critical systems 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. Systems and programs that have been added or modified since the last inspection will be reviewed as part of the current inspection. If changes to the program have not been implemented, then the inspector should select at least three systems, including one safety-related, or important-to-safety system, and one security system, to review their current implementation.

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 use the Cybersecurity Issues Forum (SIF) process. Findings and issues related to this IP shall be processed through the SIF.

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 03.05 constitute the areas in this procedure that include the inspection requirements. If a licensee develops performance testing or performance metrics as described in Section 03.06, and found satisfactory through review by the inspector, 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 03-06 and associated documents mentioned below shall describe the standards for determining satisfactory demonstration.

03.01 Review Ongoing Monitoring and Assessment Activities

a. Review Ongoing Monitoring Activities

Review the process established by the licensee to conduct ongoing monitoring and assessments. Verify that the licensee conducts assessments required by the CSP. The inspection of this control should be evaluated as complete, based on the successful conduct of license performance testing.

Specific Guidance:

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

b. Review Effectiveness Analysis

Verify that the licensee conducts an appropriate effectiveness analyses as specified in the CSP. The review requires an evaluation of the cybersecurity program and the required controls, but 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 license performance testing.

Specific Guidance:

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, controls, and program elements. Reviews of the cybersecurity program and controls include, but are not limited to, periodic audits of the physical security program, security plans, implementing procedures, cybersecurity programs; safety/security interface activities, and the testing, maintenance, and calibration program as it relates to cybersecurity.

c. Review Vulnerability Assessment Activities

Verify that the licensee performs vulnerability assessments or scans as described by the CSP, including the capability to correct exploited weaknesses. The inspection of this control should be evaluated as complete, based on the successful conduct of license performance testing.

Specific Guidance:

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 threats.

03.02 Verify Defense-in-Depth Protective Strategies

a. Defense-in-Depth Protective Strategies

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 inspection of this control should be evaluated as complete, based on the successful conduct of license performance testing.

Specific Guidance:

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., 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.

b. Defensive Security Architecture

Verify that the licensee maintains controls and elements to ensure boundary protection for the cybersecurity levels and ensures that integrity of data is maintained. 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 license performance testing.

Specific Guidance:

Licensees have implemented and documented a multi-level security defensive architecture that establishes the required level of cybersecurity. The licensee may have separated their levels by security boundary devices, such as firewalls, air gaps, or deterministic devices, through which digital communications are 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.

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 establishing the logical, and physical boundaries to control the data transfer between boundaries and between devices.

Verify that the licensee has analyzed digital computer 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.

c. Maintain Security Controls

Verify that the licensee maintained the implemented security controls to provide high assurance that the CDAs are continuously protected against cyberattacks.

Specific Guidance:

Verify that the licensee is verifying and validating that the implemented security controls are implemented correctly, operating as intended, and continuing to provide high assurance that CDAs are protected against cyberattacks up to and including the DBT.

d. User Identification and Authentication

Verify that the licensee has established access controls, and authentication and user-identification capabilities. Portions of the inspection of this control should be evaluated as complete, based on the successful conduct of license performance testing.

Specific Guidance:

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 Regulatory Guide 5.71, Appendix B.4, “Identification and Authentication”). The licensee also has policies and procedures for the periodic review of the access authorization list.

e. Portable Media and Mobile Devices

Verify that the licensee has continued to control portable media and mobile devices in accordance with the CSP. The inspection of this control should be evaluated as complete, based on the successful conduct of license performance testing.

Specific Guidance:

Licensees utilize portable media and mobile devices to update software and manage changes to CDAs. Verify that licensees have established policies and procedures that describe the control, update, and use of portable media, and mobile devices. Mobile devices should be hardened in accordance with the requirements of the CSP.

03.03 Review of Configuration Management and Change Control

a. Design Changes or Replacement Equipment

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

Specific Guidance:

Licensees typically include requirements to review CDAs as part of their existing configuration management processes and plant procedures. 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 inspector should verify that the implemented controls meet the requirements in the CSP.

b. Security Impact Analysis of Changes and Environments

Verify that the licensee performs a security impact analysis prior to making changes to CDAs to manage the cyber risk resulting from the changes. Portions of the inspection of this control should be evaluated as complete, based on the successful conduct of license performance testing.

Specific Guidance:

A cybersecurity impact analysis is performed prior to making a design or configuration change to a CDA, or when changes to the environment occur. The licensee evaluates changes to the required controls based on the assessment of the changes to manage risks introduced by the changes. The licensee assesses the interdependencies of other CDAs or support systems and incorporates the assessment into the cybersecurity impact analysis.

c. **Supply Chain and Services Acquisition**

Verify that the licensee has implemented appropriate supply chain and services acquisition controls for replacement CDAs.

Specific Guidance:

Since many replacements for CDAs will be purchased off-the-shelf, a review of supply chain and acquisition controls should be performed, and the replacement CDAs should be hardened. This review should factor in the classification of the CDA and the risk to the plant.

03.04 Review of Cybersecurity Program

a. **CSP Changes and Implementing Procedures**

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). Verify that the licensee performs activities in accordance with their implementing procedures.

Specific Guidance

The licensee will have a change procedure and licensing basis administrative controls for changing their CSP. Further, the CSP required 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.

b. **Review Incident Response and Contingency Plans**

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.

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.

Observe a licensee-conducted Cybersecurity Incident Response drill to ensure that site-defined tests or drills are used, that staff are aware of their roles and responsibilities, and that results of the drill are evaluated and documented.

c. **Review Training**

Verify that the licensee has established training as described in the CSP.

Specific Guidance:

Verify that appropriate facility personnel, including contractors, are aware of cybersecurity requirements, and receive the training necessary to perform their assigned duties, and responsibilities.

03.05 **Evaluation of Corrective Actions**

Verify that the licensee is identifying issues related to the cybersecurity program at an appropriate threshold, entering them in the CAP, and resolving the issues for a selected sample of problems associated with the cybersecurity program.

Specific Guidance:

The CSP specifies that the licensee will use the site CAP to:

1. track, trend, correct, and prevent recurrence of cybersecurity failures and deficiencies, and

2. evaluate and manage cyber risks.

Refer to IP 71152, "Identification and Resolution of Problems," for additional guidance. Ten percent of the sampling should be focused on how the licensee is addressing problems and resolutions. This can include follow-up of corrective actions for previous performance deficiencies.

03.06 Evaluation of Performance Testing or Performance Metrics

a. **Performance Testing**

Performance testing is a key element of most information technology program assessment programs. The licensee performance testing program would provide the licensee 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, 03-01b, 03.02.a, and 03.02.e. Additionally, the performance testing demonstration and information reported may satisfy portions of 03.02.b, 03.02.d, 03.03a, 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 on-site inspection should be performed to assess these controls.

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. 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 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.

   Specific Guidance:

   The observed performance test will be conducted at least 120 days before the start of the first on-site 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.

   Note: Currently a licensee is developing a draft performance testing procedure. Once that procedure or any other licensee performance testing procedure is finalized and determined by the NRC as acceptable for use, Inspectors shall refer to the licensee performance testing procedure for guidance related to determining whether the licensee had implemented authentic and realistic performance and function tests, which will include evaluation, and acceptance criteria. Items to consider include (1) confirming that the fidelity between the actual and test configurations was reasonable and (2) verifying that the licensee performed testing that challenged the network capabilities. The licensee will be given credit for the controls demonstrated by conduct of performance testing, if the guidance of the licensee performance testing procedure is adequately implemented and will be notified of this credit and of the reduction of one assigned inspector for the onsite inspection activity within 30 days of the completion of the testing.

   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 a 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 inspectors 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 portable mobile media device 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”

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

Regulatory Guide 5.83, “Cybersecurity Event Notifications” (ML14269A388)(Package ML15188A548)

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

Site Cybersecurity Plan

NEI 08-09, “Cybersecurity Plan for Nuclear Power Reactors,” Revision 6, (ML101180437); Addendum 1 (ML17079A379); Addendum 2 (ML17212A634); Addendum 3 (ML17237C076); Addendum 4, (ML17212A635), Addendum 5 (ML18226A007), Addendum 7 (ML18348B211)

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

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

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

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

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

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

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

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

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

SFAQ	Title	Accession #
10-05	IT Functions for the Critical Group	ML102100070
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
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

Attachment 1: Revision History for IP 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