CYBER SECURITY

PROGRAM APPLICABILITY: Inspection Manual Chapter 2201, Appendix A

CORNERSTONE: Security

INSPECTION BASES: See Inspection Manual Chapter (IMC) 0308, Attachment 6, "Basis Document for Security Cornerstone of the Reactor Oversight Process"

SAMPLE REQUIREMENTS:

Sample Requirements		Minimum Baseline Sample Completion Requirements		Budgeted Range	
Sample Type	Section(s)	Frequency	Sample Size	Samples	Hours*
Cyber Security	03.01 – 03.06	Biennial	1 per site	1	70 +/- 7

* see paragraph 71130.10-06

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 cyber attacks in accordance with Title 10 of the *Code of Federal Regulations* (CFR) 73.54 and the U.S. Nuclear Regulatory Commission (NRC) - approved cyber security plan (CSP).

01.02 To provide assurance that CSP changes and reports support nuclear safety and security.

71130.10-02 GENERAL GUIDANCE

02.01 Background

Evaluation of the CSP implementation occurred in three distinct phases prior to development of this cyber security baseline inspection. Initial inspections in accordance with Temporary Instruction 2201/004, "Inspection of Implementation of Interim Cyber Security Milestones 1-7," verified licensees established a qualified cyber security assessment team, identified all critical systems and critical digital assets (CDAs), effectively implemented a network architecture to separate higher cyber security 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 cyber security 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 cyber security programs. The full implementation 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. NEI 13-10, "Cyber Security Control Assessments," Revision 6, streamlined the process for addressing the application of cyber security controls to many CDAs. Industry issued addendums to NEI 08-09, "Cyber Security 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 reduce the number 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 Cyber Security Rule," and NEI 13-10 changed.

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 inspectors should select at least three systems, including one safety 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. Inspector(s) should review Security Frequently Asked Questions (SFAQs) related to cyber security requirements in advance of inspections. If the inspector(s) require policy interpretation or program clarification, then they should use the Security 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 cyber attack. Verify that the licensee is maintaining a cyber security program in accordance with its CSP and 10 CFR 73.54. The inspector(s) 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 inspectors, identified sections may be waived, as described in this inspection procedure.*

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. Information to complete this inspection step may be provided by the results of licensee performance testing.

Specific Guidance:

Ongoing assessments and monitoring activities are performed to verify that the cyber security controls implemented for critical digital assets remain in place. The assessment process verifies the licensee implements cyber security controls at the frequency specified in individual controls.

b. 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. Information to complete this inspection step may be provided by the results of licensee 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 when the licensee implements remediation as required to maintain adequate defense-in-depth protective strategies. Dispositioning includes implementation, as necessary, of cyber security controls to mitigate newly reported or discovered vulnerabilities and threats.

c. Review Effectiveness Analyses

Verify that the licensee conducts an appropriate effectiveness analyses as specified in the CSP. The review requires an evaluation of the cyber security program and the required controls at least every 24 months or at the frequency specified in the CSP.

Specific Guidance:

The effectiveness analysis ensures that the cyber security controls are implemented correctly, operating as intended, and continuing to provide high assurance that CDAs are protected against cyber-attacks up to and including the design basis threat (DBT). Reviews of the cyber security program and controls include, but are not limited to, periodic audits of the physical security program, security plans, implementing procedures, cyber security programs; safety/security interface activities, and the testing, maintenance, and

calibration program as it relates to cyber security.

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 cyber security threats. Information to complete this inspection step may be provided by the results of licensee 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 cyber-attacks on CDAs in near real-time. The defensive strategy establishes controls to ensure that the licensee can detect, delay, respond to, and recover from malware and cyber-attacks. The controls may differ for the different cyber security defensive levels. Licensees may have implemented automatic mechanisms to capture logs and to generate alarms, as necessary.

Provide defense-in-depth protective strategies through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure effectiveness of the program.

Defense-in-depth protective strategies must provide high assurance of adequate protection against adverse impact to SSEP functions resulting from cyber-attacks, which could adversely impact the integrity or confidentiality of data or software, deny access to systems, services, or data, and adversely impact the operation of systems, networks, and associated equipment to protect against the DBT.

b. Defensive Security Architecture

Verify that the licensee maintains controls and elements to ensure boundary protection for the cyber security 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. Information to complete this inspection step may be provided by the results of licensee performance testing.

Specific Guidance:

Licensees have implemented and documented a multi-level security defensive architecture that establishes the required level of cyber security. 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 critical digital assets 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.

Analyze digital computer and communications systems and networks and identify those assets that must be protected against cyber-attacks to preserve the intended function of plant systems, structures, and components within the scope of the cyber security rule and account 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 cyber attacks.

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 cyber attacks 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. Information to complete this inspection step may be provided by the results of licensee performance testing.

Specific Guidance:

The licensee has established access controls to limit and to control the access to CDAs, as prescribed by the CSP. The licensee has established policies and procedures as required by 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 removal of personnel from having access when their job functions no longer require access and 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. Information to complete this inspection step may be provided by the results of licensee 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.

f. Maintain Defense-in-Depth Protective Strategies

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

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 cyber attacks up to and including the DBT.

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 cyber-attacks. Information to complete this inspection step may be provided by the results of licensee performance testing.

Specific Guidance:

Licensees typically include requirements to review CDAs as part of their existing configuration management processes and plant procedures. They also include requirements to assess and configure CDAs for safety-related components. The licensee incorporates the control of modifications to CDAs to ensure that the they continue to be protected against cyber-attacks and meet the requirements of their CSP.

Changes to CDAs are controlled using design control or configuration management procedures so that additional cyber security 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. Information to complete this inspection step may be provided by the results of licensee performance testing.

Specific Guidance:

A cyber security 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 cyber security 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 Cyber Security 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 Cyber Security Incidents, including effectively implementing their reporting requirements.

Specific Guidance:

Identification, detection, and response to cyber-attacks are typically directed by site procedures that govern response to plant events. When there is reasonable suspicion of a cyber-attack, procedures direct notification to responsible individuals and activation of the Cyber Security Incident Response Team, as well as other emergency response actions, if warranted.

If a cyber security 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.

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 cyber security 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 cyber security program at an appropriate threshold, entering them in the CAP, and resolving the issues for a selected sample of problems associated with the cyber security program.

Specific Guidance:

The CSP specifies that the licensee will use the site CAP to (1) track, trend, correct, and prevent recurrence of cyber security 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. 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 sample takes the place of inspection requirements as determined by the type and scope of the testing. The planned performance and function testing is anticipated to demonstrate Inspection Requirements 03.02.a, 03.02.b, 03.02.c, and portions of 03.01.a, 03.01.b, 03.01.c, 03.02.d, 03.03 a, and 03.03.b. If the performance test(s) demonstrate implementation of these performance requirements, although not required, the inspection team may still elect to sample the requirements listed, above.

If the licensee elects to demonstrate performance and function test(s), verify that the performance and function testing reflects the onsite cyber system physical configuration and performance. If the answer to the following are “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 cyber security programs and cyber security 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 cyber-attack 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 cyber-attack testing performed, and realistically challenged the virtual network.

   Specific Guidance:

   The performance test will be conducted at least 120 days before the start of the first onsite week of inspection. 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: Refer to ML0000000 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 informed of the NRC's decision to credit the testing and the reduction in assigned inspectors as part of the RFI process, before the on-site inspection begins.

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 cyber security program through random testing of cyber security intrusion monitoring tools, periodic functional testing, and vulnerability scans/assessments. Therefore, the results of the licensee's performance testing shall not be documented in the inspection report in accordance with the 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, this information provided by the licensee 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 cyber security program. In accordance with the CSP, licensees are required to confirm information, document results, and evaluate the effectiveness of existing cyber security programs and cyber security controls. [A3.1.2]

Specific Guidance:

If the following data is provided completely to the inspection team during the RFI submission, the inspection team shall be reduced by contractor. The licensee will be informed of the NRC's decision to credit the performance metrics submission and of the reduction in contractors visiting the site as part of the RFI before the on-site inspection begins.

1. **Access control**

- Number of violations of access control policy identified during the quarter (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] – This value is used to evaluate the effectiveness of the access control policy and associated controls in D.1.1.

0=Good performance,
1-2=Licensee needs to investigate and make appropriate corrective actions
3 or more= Licensee needs to investigate, make appropriate corrective actions and adjust program to eliminate future performance deficiencies

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

  In accordance with CSP =Good performance
  Not in accordance with the CSP =Licensee needs to investigate and make appropriate corrective actions

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

  0-1= Good performance
  2 = Licensee needs to be investigated and make appropriate corrective actions
  3 or more = Licensee needs to investigate, make appropriate corrective actions, and adjust system program to eliminate future performance deficiencies

- 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.

  0-1 = Good performance
  2 =Licensee needs to investigate and make appropriate corrective actions
  3 or more= Licensee needs to investigate, make appropriate corrective actions and adjust program to eliminate future performance deficiencies

2. **Flaw Remediation**

- Number of security flaws not corrected (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] – This value informs the effectiveness of the technical evaluation and testing of recommended flaw remediation.

  0-1 =Good performance,
  2-3=Licensee needs to investigate and make appropriate corrective actions
  4 or more= Licensee needs to investigate, make appropriate corrective actions and adjust program to eliminate future performance deficiencies

3. **Configuration Management**

- 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 (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. [E10.3, E10.4]

  0-1 =Good performance,
  2-3=Licensee needs to investigate and make appropriate corrective actions
  4 or more= Licensee needs to investigate, make appropriate corrective actions and adjust program to eliminate future performance deficiencies

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

  0-1 =Good performance,
  2-3=Licensee needs to investigate and make appropriate corrective actions
  4 or more= Licensee needs to investigate, make appropriate corrective actions and adjust program to eliminate future performance deficiencies

- 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.

  0 =Good performance,
  Greater than 0 to 1%=Licensee needs to investigate and make appropriate corrective actions
  Greater than 1%= Licensee needs to investigate, make appropriate corrective actions and adjust program to eliminate future performance deficiencies

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]
  0-1 =Good performance,
  2-3=Licensee needs to investigate and make appropriate corrective actions
  4 or more= Licensee needs to investigate, make appropriate corrective actions and adjust program to eliminate future performance deficiencies

- Maintain the capability for the timely detection and response to cyber-attacks. Timely detection of cyber-attacks is required in order for licensees to meet CSP and regulatory requirements to mitigate and recover from cyber-attacks and to report to the NRC the results of those attacks. As a result of testing intrusion detection systems, drills, and actual events, has the licensee determined the mean time to respond and to report? [10 CFR 73.54, 10 CFR 73.77, E3.4, E3.6]
  Less or equal to one hour =Good performance,
  More than one hour = Licensee needs to investigate, make appropriate corrective actions and adjust program to eliminate future performance deficiencies

6. **Software and information integrity**

- Number of software integrity verification failures (reassessing and documenting the integrity, operation, and functions of software and information by performing regular integrity, and operation and functional scans, in accordance with the CSP. Employing and documenting automated tools, where technically feasible, that provide notification to designated individuals upon discovering discrepancies during integrity verification, employing and documenting centrally managed integrity verification tools). [E3.7]
  In accordance with the CSP =Good performance,
  Not in accordance with the CSP=Licensee needs to investigate and make appropriate corrective actions

7. **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]
  100-95% =Good performance,
  94-90%=Licensee needs to investigate and make appropriate corrective actions
  Less than 90% = Licensee needs to investigate, make appropriate corrective actions and adjust program to eliminate future performance deficiencies

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

Staff assigned =Good performance,
Staff not assigned = Licensee needs to investigate, make appropriate improvements and adjust program to eliminate future performance deficiencies

- Personnel staffing, qualifications, and training [NEI Cyber Security Program Performance Review October 2020]
  Exceeds minimum requirements = Green
  Meets minimum requirements = White
  One department does not meet minimum requirements = Yellow
  More than one department does not meet minimum requirements = Red

8. **System Hardening**

- Number of unnecessary open ports and protocols for communication for firewalls discovered and removed [E6]
  0-1 =Good performance,
  2-3=Licensee needs to investigate and make appropriate corrective actions
  4 or more= Licensee needs to investigate, make appropriate corrective actions and adjust program to eliminate future performance deficiencies

71130.10-04 RESOURCE ESTIMATE

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.

When a licensee elects to demonstrate an authentic and realistic performance and function test of the cyber security network configuration, the opportunity could provide inspectors a more efficient way to evaluate the licensee's defensive architecture and selected program elements. If the inspectors conclude that the licensee provided an effective, acceptable performance and function test, then the inspection may consist of one inspector and two contractors for one week. This resource reduction occurs because the satisfactory performance and function test provides reasonable assurance of site cyber security protection in the inspection areas identified in this procedure. As a result, the estimated time to complete the inspection procedure direct inspection effort shall be 42 hours per site (12 hours for performance and function test observation applicable to the site and 30 hours for on-site inspection with an overall range of 36 to 48 hours per site).

71130.10-05 PROCEDURE COMPLETION

The inspection of the minimum number of inspection requirements will constitute completion of this procedure. The inspection requirement range for completion is as follows: minimum three (3) inspection requirements, nominal four (4) inspection requirements, and maximum five (5) 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).

71130.10-06 REFERENCES

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

10 CFR 73.77, "Cyber Security Event Notifications"

Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities" (ML090340159)(Package ML090340152)

Regulatory Guide 5.83, "Cyber Security Event Notifications" (ML14269A388)(Package ML15188A548)

Site Cyber Security Plan

NEI 08-09, "Cyber Security 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 Cyber Security Rule," Revision 2, and NRC Letter acknowledging NEI 10-04 to be acceptable for use with exceptions (ML12180A081)

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

ML20126G492 - Endorsement of 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

ML20205L604 – Endorsement of 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

ML20199M368 – NRC Review of 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

NEI 15-09, "Cyber Security Event Notifications," (Revision 0, ML16063A063)

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

Security Frequently Asked Questions (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	Ascension #
10-05	IT Functions for the Critical Group	ML102100070
12-17	Cyber Security Milestone 1	ML13098A153
12-18	Cyber Security Milestone 2	ML13098A155
12-19	Cyber Security Milestone 3	ML13098A157
12-20	Cyber Security Milestone 4	ML13098A170
12-21	Cyber Security Milestone 5	ML12331A131
12-22	Cyber Security Milestone 6	ML13098A174
12-23	Cyber Security 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 / PADS	ML16209A095
16-05	Moving Data between Security Levels	ML16351A469
16-06	Communications Attack Pathways	ML16351A504
17-04	Access Authorization / Access Authorization Systems	ML18030A535

CYBER-SECURITY Guidance Document for Development of the Request for Information (RFI) and Notification Letter for Full-Implementation of the Cyber-Security Inspection (ML17156A215)

Licensee procedure for conducting performance-function testing ML000000000

Template for adequate performance metrics submission ML000000000

END

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		IP 71130.10 is being issued to include updates resulting from inspection feedback and revised to support realignment of Agency document standards.	None	