CYBER SECURITY

Guidance Document for Development of the Request for Information (RFI) and Notification Letter for IP 71130.10 Cyber Security Inspection

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NOTICE:

The focus of this document is to provide guidance to the NRC cyber security inspection personnel regarding the types of information typically requested, enabling the inspection team to make informed decisions when developing a site-specific cyber security inspection plan.

Issue Date: 11-22-2021

Table of Contents

1 Introduction

Both the previously conducted Milestone 1 through 7 cyber security inspections and the full-compliance (i.e., Milestone 8) “pilot” inspections, have demonstrated that a major factor impeding the ability of inspection personnel to perform their duties is the availability of relevant licensee documentation that supports or refutes the determination of compliance with a given aspect of the licensee’s Cyber Security Plan (CSP) and Title 10, *Code of Federal Regulations (10 CFR)*, “Protection of Digital Computer and Communication Systems and Networks,” Part 73, Section 54 (10 CFR 73.54). Although the practice of data-gathering site visits (i.e., bag-man trips) attempted to address this need, there remains a continuing problem of the need to search through huge amounts of documentation, which all-too-often turns out to be inadequate or non-applicable, to settle the issue of compliance with cyber security requirements. One of the related problems has been with inconsistency among the various licensees regarding the types of documentation they maintain, and the descriptions or titles used for various types of documentation. To improve the effectiveness and consistency of the data gathering process this guidance document has been developed to provide specific details about the kinds of information and data that could be requested from the licensee during the inspection preparation activities.

Return to Table of Contents

2 Overview and Purpose

This document is intended to be used as a guidance document to develop the Request for Information (RFI) and notification letter issued to licensees for implementation of the full-compliance cyber security inspection. The first round of requested information concentrates on providing the inspection team with the general information necessary to develop a site-specific inspection plan. The requested information includes the identification of critical systems (CSs) and critical digital assets (CDAs), Nuclear Energy Institute (NEI) 08-09, Revision 6, Appendix D & E controls, and programmatic CSP elements that will form the sample set for the Cyber Security Inspection Procedure (IP) 71130.10. The information requested will also aid in understanding the licensee's application of NEI 13-10 and how or if it impacts inspection planning. The inspector's review of the first round of information will result in an additional, and more focused, follow-on requests for information. The documentation listed in Section 3 is intended to be as comprehensive as possible and the inspection team may find some of the items may not be relevant or applicable to their licensee's plant and program. Therefore, the team may or may not use all or only selected parts of the documentation identified in Section 3.

In addition to providing a comprehensive list of information to be requested, this guidance document also provides descriptions (i.e., for most of the listed document types) that detail the content that is expected for each and, for some of the documents, Section 4 provides an actual example document to show the form and format of the document as it is expected to be supplied by the licensees. A primary objective of this guidance document is to establish a consistent and standardized process that aids both the licensees and NRC personnel in the identification and collection of the specific information needed to perform the cyber security inspection. Note that this document attempts to avoid assigning a specific "name" to some sets of information, and offers a description instead, since licensees may or may not use the same nomenclature for the requested information.

The table below, "Sequence of Request for Information," specifies the sequence of documentation requests issued to the licensee prior to implementation of the cyber security inspection. The first RFI concentrates on providing the inspection team with the general information necessary to select appropriate components and CSP elements to develop a site-specific inspection plan. The first RFI is used to identify the list of CSs/CDAs plus operational and management (O&M) security control portions of the CSP to be chosen as the "sample set" required in the cyber security IP. The inspectors' review of the returned documentation from the first RFI will be utilized to provide a more focused follow-up request during a second RFI. Examining the returned information from the first RFI, the inspectors will identify and select specific systems and equipment (e.g., CSs/CDAs) to develop the second RFI. The second RFI will request additional information required to evaluate the CSs/CDAs, defensive architecture, and the areas of the licensee's CSP selected for the cyber security inspection.

2 Overview and Purpose

Return to Table of Contents

Section 3, Paragraph Number/Title:		IP Ref.
NRC Request for Information #1[1]		
1	A list of all Identified Critical Systems and Critical Digital Assets,– highlight/note any . additions, deletions, reclassifications due to new guidance from white papers, changes to NEI 10-04, 13-10, etc. since the last cyber security inspection.	Overall
2	A list of EP and Security onsite and offsite digital communication systems	Overall
3	Network Topology Diagrams to include information and data flow for critical systems in levels 2, 3 and 4 (If available)	Overall
4	Ongoing Monitoring and Assessment program documentation	03.01(a)
5	The most recent effectiveness analysis of the Cyber Security Program	03.01(b)
6	Vulnerability screening/assessment and scan program documentation	03.01(c)
7	Cyber Security Incident response documentation, including incident detection, response, and recovery documentation as well as contingency plan development, implementation and including any program documentation that requires testing of security boundary device functionality	03.02(a) and 03.04(b)
8	Device Access and Key Control documentation	03.02(c)
9	Password/Authenticator documentation	03.02(c)
10	User Account/Credential documentation	03.02(d)
11	Portable Media and Mobile Device control documentation, including kiosk security control assessment/documentation	03.02(e)
12	Design change/ modification program documentation and a List of all design changes completed since the last cyber security inspection, including either a summary of the design change or the 50.59 documentation for the change.	03.03(a)
13	Supply Chain Management documentation including any security impact analysis for new acquisitions	03.03(a), (b) and (c)
14	Configuration Management documentation including any security impact analysis performed due to configuration changes since the last inspection	03.03(a) and (b)
15	Cyber Security Plan and any 50.54(p) analysis to support changes to the plan since the last inspection	03.04(a)
16	Cyber Security Metrics tracked (if applicable)	03.06 (b)
17	Provide documentation describing any cyber security changes to the access authorization program since the last cyber security inspection.	Overall
18	Provide a list of all procedures and policies provided to the NRC with their descriptive name and associated number (if available)	Overall

2 Overview and Purpose

Section 3, Paragraph Number/Title:		IP Ref.
19	Performance testing report (if applicable)	03.06 (a)
NRC REQUEST FOR INFORMATION #2		
	For the system(s) chosen for inspection provide:	
1	Ongoing Monitoring and Assessment activity performed on the system(s)	03.01(a)
2	All Security Control Assessments for the selected system(s)	03.01(a)
3	All vulnerability screenings/assessments associated with or scans performed on the selected system(s) since the last cyber security inspection	03.01(c)
4	Documentation (including configuration files and rules sets) for Network-based Intrusion Detection/Protection Systems (NIDS/NIPS), Host-based Intrusion Detection Systems (HIDS), and Security Information and Event Management (SIEM) systems for system(s) chosen for inspection)	03.02(b)
5	Documentation (including configuration files and rule sets) for intra-security level firewalls and boundary devices used to protect the selected system(s)	03.02(c)
6	Copies of all periodic reviews of the access authorization list for the selected systems since the last inspection	03.02(d)
7	Baseline configuration data sheets for the selected CDAs	03.03(a)
8	Documentation on any changes, including Security Impact Analyses, performed on the selected system(s) since the last inspection	03.03(b)
9	Copies of the purchase order documentation for any new equipment purchased for the selected systems since the last inspection	03.03(c)
10	Copies of any reports/assessments for cyber security drills performed since the last inspection.	03.02(a) 03.04(b)
11	Copy of the individual recovery plan(s) for the selected system(s) including documentation of the results the last time the backups were executed.	03.02(a) 03.04(b)
12	Corrective actions taken as a result of cyber security incidents/issues to include previous NRC violations and Licensee Identified Violations since the last cyber security inspection	03.04(d)
	Information provided to the NRC at the start of the inspection	
1	Any cyber security event reports submitted in accordance with 10 CFR 73.77 since the last cyber security inspection	03.04(a)
2	Updated Copies of corrective actions taken as a result of cyber security incidents/issues, to include previous NRC violations and Licensee Identified Violations since the last cyber security inspection, as well as vulnerability-related corrective actions	03.04(d)

Notes:

[1] This table does not address the full set of O&M and technical controls in Regulatory Guide (RG) 5.71, nor NEI 08-09, Revision 6, nor all of the CSP areas enumerated in the Cyber

2 Overview and Purpose

security IP. Additional information requests may be made for those items not addressed in the table once the inspection team has finalized the inspection plan and during the onsite inspection.

Return to Table of Contents

3 Initial Documentation Requests – RFI #1

The following information should be requested from licensees as early in the inspection planning process as possible, preferably as part of the formal “120 day” inspection notification letter, and should be used to guide the inspection team’s decisions regarding focus areas for development of the site-specific inspection plan.

1. A list of all Identified Critical Systems and Critical Digital Assets,– highlight/note any additions, deletions, reclassifications due to new guidance from white papers, changes to NEI 10-04, 13-10, etc. since the last cyber security inspection

    a. For each CDA, and non-CDA cyber defensive digital asset provide the following information in a tabular format using an Excel spreadsheet workbook with a column for each of the following items of information:
        1) Plant Identification (ID) and/or Designation (e.g., Equipment ID Number (EIN), Equipment Part Number (EPN), system name, etc.);
        2) Safety, Security, and Emergency Preparedness (SSEP) Function/Designation (i.e., Safety, Important to Safety, Security, or Emergency Preparedness);
        3) Any associated CS of which this CDA or digital asset is an element;
        4) Type of Component (e.g., flow, pressure, or level transmitter/programmable logic controller (PLC)/recorder, etc.);
        5) Manufacturer;
        6) Model Number;
        7) Software/Firmware Version Number(s);
        8) Physical Location (locations if digital asset is composed of multiple elements);
        9) Plant Cyber security Level (Level 1 – 4 or Not Networked) declared for the digital asset;
        10) Critical Digital asset LAN ID or designation, if applicable;
        11) If the CDA has been categorized using the NEI 13-10 approach, then include its direct (e.g., A.1 through B.4, if appropriate) or indirect (e.g., indirect, Emergency Preparedness (EP), Balance-of-Plant (BOP) or BOP-Trip) classification where applicable;
        12) Brief description of the SSEP function the CDA performs (i.e., what makes the digital asset qualify as a CDA);
        13) Network Drawing or Diagram Number (Also provide a portable document format (pdf) drawing or diagram); and
        14) Network Type, if digital asset is network connected (e.g., TCP/IP, DECNet, NovelNet (IPX/SPX), IBM Systems Network Architecture (SNA), Token-Ring, SONET, Asynchronous Transfer Mode (ATM), Fiber Distributed Data Interface (FDDI) and vendor-proprietary LANs such as Modbus+ and DataHighway/DataHighway+); and
        15) All subsystems/support systems upon which this CDA depends

Return to Request for Information #1

3 Initial Documentation Requests – RFI #1

2. List EP and Security onsite and offsite digital communications systems

[Note: Potential Safeguard Information (SGI) Designation]

a. Provide a list of EP and Security onsite and external/off-site digital communications systems and devices either designated as CDAs or associated with SSEP functions as follows:

1) Include all digital communications systems and devices designated as CDAs or associated with or supporting SSEP functions. Examples of onsite and external/offsite digital communications systems and devices include:
   i. Portable and base-station digital radios (security and non-security) including repeaters;
   ii. Digital and/or Voice over Internet Protocol (VoIP) phone systems;
   iii. Digital private branch exchanges (PBXs);
   iv. Fax machines and associated analog phone lines;
   v. Digital microwave links to other sites;
   vi. Satellite phones; and
   vii. Cellular phones (exclude personal cellular phones).

2) For each onsite and offsite digital communication system and/or CDA device provide the following:
   i. Plant ID and/or Designation (e.g., EIN, EPN, etc.);
   ii. Any associated CSs or CDAs;
   iii. Make;
   iv. Manufacturer;
   v. Model-Number;
   vi. General overview and description of its SSEP (or SSEP support) functions;
   vii. Physical Location;
   viii. Security level (1 through 4) assigned to the system/device; and
   ix. Any in-plant and external network connections to the system/device or communication channels interfaced with the system/device.

NOTE – During the onsite inspection, a detailed list of onsite and offsite digital communications systems and devices will be required. Due to the SGI nature of the list, a highly simplified and less information-rich version that does not constitute SGI would be adequate for the initial round of information gathering.

Return to Request for Information #1

3 Initial Documentation Requests – RFI #1

3. Network Topology Diagrams to include information and data flow for critical systems in levels 2, 3 and 4 (If available) (be sure to include all Network Intrusion Detection System/Network Intrusion Prevention (NIDS/NIPS) and Security Information and Event Management (SIEMS) for EP networks and Security level 3 and 4 networks)

   a. For each LAN and or LAN segments with CDAs on them, provide network topology diagrams which include and identify the following:
      1) LAN interconnections with fiber optic, copper and wireless routes;
      2) Identify all NIDS/NIPS and SIEMS locations for EP networks and Security level 3 and 4 networks.
      3) Logical and physical placement of network elements, components and network members;
      4) Physical and network address information including subnet designations;
      5) Data and information flow control;
      6) Network components that have spare and/or unused interfaces (e.g., an Ethernet switch with unused ports);
      7) For network elements that incorporate rules that block selected message traffic (e.g., switches, routers, firewalls, etc.) or that control the routing of message traffic (e.g., routers, switches) clearly identify this functionality on the diagram either through the use of standard symbols (e.g., Cisco symbol library) or explanatory text;
      8) Spare and/or unused interfaces that are disabled via administrative (i.e., configuration settings) and/or by physical means;
      9) Network components and/or elements that have a local-access interface (e.g., a “console port”) that are disabled via administrative (i.e., configuration settings) and/or by physical means; and
      10) As an alternative, if the specific detailed information for the various network components (e.g., disabled, spare and console ports on a switch) are not on the available network drawings, but are provided on other related documents, then include those other documents as well. Refer to Section 4 for an example of a network topology diagram.

Return to Request for Information #1

3 Initial Documentation Requests – RFI #1

4. Ongoing Monitoring and Assessment program documentation

   a. Provide documentation to support the ongoing monitoring and assessment (OM&A) program which includes the following ongoing and monitoring procedures for:
      1) Configuration management of CDAs
      2) Cyber security impact analyses of changes to CDAs or their environments to ensure cyber security controls are performing effectively
      3) Ongoing assessments to verify that Ongoing assessments to verify that the cyber security controls implemented for CDAs remain in place throughout the life cycle of the CDA;
      4) Verification that rogue assets are not connected to the network infrastructure
      5) Ongoing assessments of the need for and effectiveness of the cyber security controls identified in Appendices D and E of NEI 08-09, Revision 6; and
      6) Periodic cyber security program review to evaluate and improve the effectiveness of the Program.
   b. List of automated support tools used for OM&A

Return to Request for Information #1

3 Initial Documentation Requests – RFI #1

5. Most recent Effectiveness analysis of the Cyber Security Program

   a. Provide the most recent effectiveness analysis of the cyber security program, including documentation that:
      1) Provides insight for improving performance of the Cyber Security Program;
      2) Assists in determining the effectiveness of cyber security controls in Appendices D and E of NEI 08-09, Revision 6;
      3) Assists in ascertaining whether specific cyber security controls are functioning and are helping facilitate corrective action prioritization; and
      4) Illustrates the fusion of Cyber Security Program activities data with the data obtained from automated monitoring and evaluation tools in a manner that can be tied to cyber security control implementation.

Return to Request for Information #1

3 Initial Documentation Requests – RFI #1

6. Vulnerability screening/assessment and scan program documentation

   a. Provide information on the licensee vulnerability screening and assessment process, including
      1) Procedures for acquiring, reviewing, screening, and assessing security alerts and advisories
   b. Provide information on the licensee vulnerability scanning and assessment process, including:
      1) Procedure for determining which assets are scanned and which are assessed
      2) Procedure for vulnerability scanning, including periodicity
      3) Procedures for non-scan assessments
      4) Examples of recent vulnerability assessments

Return to Request for Information #1

3 Initial Documentation Requests – RFI #1

7. Cyber Security Incident response documentation (including incident detection, response, and recovery documentation as well as contingency plan development and implementation and also including any testing of security boundary device functionality)

   a. Provide program documentation for Cyber Security Incident response include procedures that provide guidance for the following
      1) Incident detection
      2) Incident response
      3) Incident recovery
      4) Contingency plan development and implementation
      5) Requirements for testing security boundary device functionality

Return to Request for Information #1

3 Initial Documentation Requests – RFI #1

8. Device Access and Key Control documentation

   a. Provide the device access and key control procedure(s) that document the use of physical security measures and controls (e.g., locked enclosures and/or cabinets, key-card access-controlled and/or alarmed rooms, etc.) used to monitor and control physical access to CSs and/or CDAs.
   b. For the procedure(s) provided the appropriate section(s) shall be identified and marked (i.e., highlighted) that explain the processes which:
      1) Describes the process used to authorize, issue, and track the use of physical keys and lock combination numbers for personnel that have access authority for the various CDAs;
      2) Describes the access differentiation levels and/or location (e.g., site, building, area, and room) provided by the access control system and the logging performed on key-card access events; and
      3) Describes the access review process and periodicity and information sources (e.g., key checkout log, access monitoring system log, video surveillance, etc.) available for auditing physical access to the associated CSs and/or CDAs.

Return to Request for Information #1

3 Initial Documentation Requests – RFI #1

9. Password/Authenticator documentation

   a. Provide the password/authenticator policy procedure(s) that address the full range of password-based access controls and non-password authentication methods employed at the site including for CSs/CDAs, where password strength and complexity may be technically limited (e.g., a six-digit number) or where physical authenticators (e.g., a key, a combination or electronic fob/dongle) are employed to control access.
   b. For the procedure(s) provided the appropriate section(s) shall be identified and marked (i.e., highlighted) that explain the process which:
      1) Specifies the time periodicity and/or conditions (or events) under which passwords and/or authenticators would be changed;
      2) Specifies the requirements for selecting passwords for the full range of password types supported by CSs and/or CDAs;
      3) Specifies what types of authenticators are acceptable and the criteria for selecting;
      4) Specifies the approved alternative countermeasures that can be used in cases where a CS and/or CDA does not support passwords or authenticators, especially where password or authenticator use could pose a safety or security risk;
      5) Addresses identifying and replacing factory/default passwords on CSs and/or CDAs;
      6) Addresses actions to be taken if a CS's and or CDA's user-access password or authenticator is compromised or suspected of being compromised, particularly when a group of personnel "share" a single, universal password; and
      7) Describes the issuance and revocation of authenticators, including the approvals required, the periodicity review, and any events that would trigger a review.

Return to Request for Information #1

3 Initial Documentation Requests – RFI #1

10. User Account/Credential documentation

a. Provide the user account/credential policy and account review procedure(s) that address the full range of account-based access controls employed at the site including for CSs/CDAs where account-based user differentiation is either quite limited (i.e., a small, fixed number of access levels) or not technically supported (e.g., no passwords/accounts or a single, universally-used password with no specific account/user association).

b. For the procedure(s) provided the appropriate section(s) shall be identified and marked (i.e., highlighted) that explain the process which:
   1) Specifies the time periodicity and/or conditions under which user accounts on CSs and/or CDAs would be reviewed, changed or removed;
   2) Specifies the approval and review process used for authorizing personnel to have user access to CSs and/or CDAs and particularly “root” or “admin” access;
   3) Specifies the approved alternative countermeasures that may be used in cases where a CSs and/or CDAs does not support user accounts or where use of user accounts would pose a safety or security risk;
   4) Addresses identifying and eliminating factory/default, support and guest accounts on CSs and/or CDAs;
   5) Addresses actions to be taken if a user-account is compromised or suspected of being compromised;
   6) Includes the requirements for qualifying personnel to have accounts on the various types of CSs and/or CDAs;
   7) Defines the criteria for determining which access level is appropriate for a given job description and/or role, where access level differentiation is supported on a CS and/or CDA;
   8) Specifies the process used to ensure secure transmission of credentials; and
   9) Provides justification for any case in which a CS and/or CDA and or associated system technically supports all of the user account protective requirements specified in NEI 08-09, Revision 6, Appendix D, Sections 1.1 through 1.10, but the licensee has elected not to implement some or all of those functions

Return to Request for Information #1

3 Initial Documentation Requests – RFI #1

11. Portable Media and Mobile Device control documentation

a. Provide the portable media and mobile device (PMMD) control procedure(s) or description of licensee processes that detail the methodology used to control PMMDs that are within the scope of the CSP, but are not included as Measurement and Test Equipment (M&TE). (That is covered in section 13)

b. For the procedure(s) or description of licensee processes provided the appropriate section(s) shall be identified and marked (i.e., highlighted) that explain the processes which:
   1) Address the custody transfer process;
   2) Address the associated documentation tracking process (e.g., a labeling and numbering scheme);
   3) Address the audit process;
   4) Describes the process used to move digital data from the source to the PMMD and then to a CS and/or CDA;
   5) Describes the authority to physically control, store, issue, and retain PMMD;
   6) Describes the transfer of PMMD information (e.g., data files, programs, etc.) to and/or from a CS and/or CDA;
   7) Describes the process used to verify PMMD integrity and ensures that PMMD do not contain malicious software which could be used as a cyber-attack pathway;
   8) Identifies the responsible individual and or organization that has the authority to be in possession of PMMD;
   9) Explains, in technical detail, the process and technologies (e.g., anti-virus (AV) scanning software on a “kiosk”) used for device (i.e., firmware, software, configuration settings, etc.) and device content integrity verification, including security control assessment or other documentation that describes:
      i. The physical security controls, (e.g., cabinets, port blockers)
      ii. The technical security controls used to protect the integrity of the process or technology, (e.g., system hardening, malware detection, logical access control;)
      iii. The operational controls used to ensure correct and authorized operation of the process or technology
   10) Explains the process of field updating of firmware used for obtaining, validating, and installing firmware updates; and
   11) Addresses by what means PMMD are uniquely identified for tracking and auditing purposes and how specific devices are associated with security levels and or specific CSs and or CDAs.

c. Provide a list of “Smart” portable computer-readable media. For example, a USB thumb drive with a password, file management functionality and or encryption capabilities. Do not include PM that is unable to change their contents (e.g., a CD or magnetic tape) or passive (e.g., a memory stick or dumb USB “thumb drive”).

3 Initial Documentation Requests – RFI #1

d. Provide a list of:
   1) Any PMMDs that are specifically excluded from the scope of the CSP and the justification for being excluded;
   2) Any prohibited PMMDs (e.g., “Wi-Fi hot spots”) or PMMDs that are restricted and the specifics of the restrictions (e.g., no cell phones or cameras in rooms, where SGI is discussed); and
   3) All personnel who are authorized to perform firmware updates.

Return to Request for Information #1

3 Initial Documentation Requests – RFI #1

12. List all design changes completed since the last inspection including 50.59 documentation and the design change/modifications program documentation

    a. Provide program documentation for how a design change/ plant modification is performed.
    b. Provide a list of all the design changes performed since the last cyber security inspection
    c. Provide either a summary paragraph that explains the design change or a copy of the 50.59 evaluations that were performed as well as any supporting information (e.g., work order documenting the 50.59 evaluation, etc.)

Return to Request for Information #1

3 Initial Documentation Requests – RFI #1

13. Supply Change Management program documentation including any security impact analysis for new acquisitions since last inspection

    a. Provide the supply chain management procedure(s) that document the methodology used to purchase new systems and services and comply with the facilities CSP, specifically how the licensee:
        1) Maintains Custody and Control of devices or Software from a Vendor to Installation
        2) Guidance for the establishment of trusted distribution paths
        3) How vendors are validated
        4) Requirements for tamper proof devices on acquired products
    b. Provide documentation on how the licensee ensures that acquired products meet defined levels of trustworthiness and how the licensee ensures that software developers employ software quality and validation methods to minimize flawed or malformed software.
    c. How the licensee ensures that new acquisitions integrate security capabilities into newly acquired devices including:
        1) Ensuring the procurement of CDAs is informed by the vulnerability and threat management program
        2) Either the Supplier or the licensee performs a Security Impact analysis to consider how assets could be exploited and the potential impacts of security control failures on CDA security and safety functions.
    d. How the licensee requires that system developers/integrators create a security test and evaluation plan, implement the plan, and document the results
    e. Documentation on required licensee testing need prior to installation.
    f. Documentation of audits required by the licensee's CSP to validate the following items:
        1) Security controls present during system validation testing are still installed and operating in the production system
        2) CDA are free from known security compromises
        3) Management change program is being followed with an audit trail of review and approvals for changes

Return to Request for Information #1

3 Initial Documentation Requests – RFI #1

14. Configuration Management documentation to include any security impact analysis performed due to configuration changes since the last inspection

    a. Provide a high-level explanation of the processes and procedure(s) that govern and control configuration changes to CDAs.
    b. Provide a list of plant modifications to CDAs for which cyber security program elements have been added, deleted, or modified and the associated assessment that was performed in accordance with the licensee's CSP
    c. Provide configuration management procedure(s), including Hardware/Software/Firmware, that establish, approve, document, and verify CDA "hardware configuration." The CDA "hardware configuration" refers collectively to the CDA-supported options and variations, CDA software and/or firmware complement, including 3rd-party applications and software additions, and essential CDA configuration value settings.
    d. For the procedure(s) with references provided the appropriate section(s) shall be identified and marked (i.e., highlighted) that explain how the processes below were addressed :
        1) Establish the initial baseline CDA "hardware configuration" and any subsequent change(s);
        2) Defines individuals that have authorization to make changes to any and/or all of the elements;
        3) Establishes specialized training requirements for those individuals and how such changes are verified, tracked and audited;
        4) Evaluates, documents and implements changes to hardware or software or configuration settings;
        5) Ensures any implemented changes do not introduce new vulnerabilities, malicious, unauthorized, altered functionality; and
        6) Ensures proposed changes to CDAs are evaluated to ensure that the CDA's cyber protections remain effective and adequate.
    e. Provide a high-level explanation of the processes and procedure(s) that documents, and maintains an inventory of the components of CDAs
    f. Provide the inventory management and control procedure(s) that address the tracking, identification and control of CDAs, and their components (e.g., Storage devices, video cards, Motherboards, Network Interface Adapters, PLCs and their associated communication and I/O modules, etc.) (if available).
    g. For the procedure(s) provided the appropriate section(s) shall be identified and marked (i.e., highlighted) that address the tracking, identification and control of CDAs, and their components as follows:
        1) Identify components of systems/devices to a detail level sufficient to account for knowing which systems/devices may be due or eligible for an available or required software update or security patch;

3 Initial Documentation Requests – RFI #1

2) Indicate how inventory management procedures identify the software/firmware versions of all inventory components that are associated with support of CSs/CDAs

h. Include any Cyber Security Impact analysis performed due to changes in a CDA's configuration or environment to manage risks introduced by the changes since the last cyber security inspection

Return to Request for Information #1

3 Initial Documentation Requests – RFI #1

15. Cyber Security Plan and any 50.54(p) analysis to support changes to the plan since the last inspection

    a. The licensee should provide a copy of their current Cyber Security Plan (CSP).
    b. The licensee should provide copies of all 50.54(p) analyses that have been performed to support changes to the CSP since it was originally approved by the NRC.

Return to Request for Information #1

3 Initial Documentation Requests – RFI #1

16. Cyber Security Metrics (if tracked)

Licensees are required to collect, examine, and document the existing cyber security policies, procedures, and practices; existing cyber security controls; detailed descriptions of network and communication architectures (or network/communication architecture drawings); information on security devices. (NEI 08-09 Revision 6 Appendix A, Section 3.1.4)

Each of the following performance metrics are mapped to a security control that provides regulatory guidance. Metrics data shall also provide data obtained from the use of any alternate controls. Wording from NEI 08-09 is underlined in the performance metric column below.

Sample size shall be the twenty four months preceding current month or since the last inspection, which ever period is longer.

3 Initial Documentation Requests – RFI #1

1. Access Control:

Perf. Metric	Security Control(s) Highlighted	Sample Size	Measurement	Count/ Numeric Data
Number of violations of access control policy identified	**D1.1, D1.4, D1.11, and D2.6** Access Control Policy and Procedures	All instances of unauthorized access to CDAs.	The definition of an access control policy is any access control requirement in Regulations, CSP, and/or Procedures. Number of times other than authorized individuals and/or processes acting on their behalf gained access to CDAs and/or performed activities on these devices. Access control is normally controlled digitally, however, some devices may only be controlled physically. Access control measures may take different forms depending on limitations. (This is an example of this metric reporting: A digital device which is rudimentary and does not have logging capabilities nor is capable of supporting IDS, is controlled through physical security controls and is locked and signed out only to authorized personnel. The Licensee would determine access control performance on these devices by reviewing the physical security control measures and reporting any violations of these measures.) Access control policy violations would normally be captured digitally in logs and audit records of SIEMs, firewalls, and IDSs. Capturing these violations through physical security processes would occur as discussed above. Note the trending, tracking, and periodicity requirements. See the	Total violations: **x**

3 Initial Documentation Requests – RFI #1

			guidance in A3.1.6, D1.1, and D2.6 If the Licensee provides the performance metric data as described here, then the Inspection Team shall determine the performance metric submission adequate.	
Manages and documents CDA accounts, including authorizing, establishing, activating, modifying, reviewing, disabling, and removing accounts	**D1.2** Account Management	All employee or contractor changes in accordance with requirements.	Report the total number of instances where the time to disable and remove user credentials of individually separated workers due to a change of duty or employment, went beyond the allotted time permitted in the requirements. Record that result in this form. (This is an example of this metric reporting: An IT engineer with administrative access to IT resources is transferred to a management position at another plant. Upon review of user credentials, it is discovered that the access control and admin rights were not changed to reflect the new job role for 50 days. The requirements for this licensee states: "Network and system access credentials will be changed as a result of any duty change or worker separation within 30 days." The preceding example shall be reported in the count of instances.) Note the trending, tracking, and periodicity requirements. See the guidance in A3.1.6 and D1.2	Number of instances exceeding requirements x

3 Initial Documentation Requests – RFI #1

			If the Licensee provides the performance metric data as described here, then the Inspection Team shall determine the performance metric submission adequate.	
Number of non-compliance incidents by third-party personnel E5.2 and D1.3	**E5.2, D1.1, D1.3, and D4.5** Access Enforcement and Third Party/Escorted Access	Total number of third-party personnel non-compliance incidents.	The definition of non-compliance is failure to comply with requirements in Regulations, CSP, and or Procedures. Total number of non-compliance (in accordance with the requirements and procedures) incidents by third-party personnel that occurred. Note the trending, tracking, and periodicity requirements. See the guidance in A3.1.6 and D1.1 The definition of non-compliance is failure to comply with requirements in Regulations, CSP, and or Procedures. Total number of non-compliance (in accordance with the requirements and procedures) incidents by third-party personnel that occurred. For those licensee's that are reporting a quantitative value for this metric of >2, provide quantitative or qualitative context as to the health of the licensee's cyber program for this control, for example: Quantitative: 5 non-compliance incidents against the total number of third-party personnel that	Non-compliance incidents: **x**

3 Initial Documentation Requests – RFI #1

			gained CDA access during the 24-month period (e.g., 150). Or, Qualitative: A COMPLETED causal analysis addressing the increased number of non-compliances. If the Licensee provides the performance metric data as described here, then the Inspection Team shall determine the performance metric submission adequate.	
Number of unauthorized PMMD connected to CDAs	**D1.18** Insecure and Rogue Connections **D1.19** Access Control for Portable and Mobile Devices	Total number of unauthorized PMMD connected to CDAs.	Report the total number of unauthorized PMMD connected to CDAs. If the Licensee provides the performance metric data as described here, then the Inspection Team shall determine the performance metric submission adequate. Note the trending, tracking, and periodicity requirements. See the guidance in A3.1.6 and D1.18 If the Licensee provides the performance metric data as described here, then the Inspection Team shall determine the performance metric submission adequate.	Unauthorized connections: **x**

3 Initial Documentation Requests – RFI #1

2. Flaw Remediation:

Perf. Metri	Security Control(s) Highlighted	Sample Size	Measurement	Count/ Numeric Data
Number of security flaws not corrected	**E3.2 and E12** Flaw Remediation	Total number of security flaws identified that were not corrected or mitigated before the CDA(s) were put into production and for the lifecycle of the CDA(s).	Security flaws, insecure configurations, and other items that could be determined to be targets for compromise may be identified by performing vulnerability scans or assessments. The definition of a security flaw is a security weakness and especially one that detracts from the whole or hinders effectiveness. Identify the total number of security flaws that have been identified but not mitigated through CSP standard or alternate controls. Record that numeric result in this form and provide the reason(s) for not correcting the flaw. It is understood that some security flaws may not be corrected because of safety or security interface requirements as per 10 CFR 73.58. Also, see NEI 08-09 Addendum 5 for additional guidance. If the Licensee provides the performance metric data as	Security Flaws not corrected: x

3 Initial Documentation Requests – RFI #1

			described here, then the Inspection Team shall determine the performance metric submission adequate.	

3 Initial Documentation Requests – RFI #1

3. Configuration Management:

Perf. Metric	Security Control(s) Highlighted	Sample Size	Measurement	Count/ Numeric Data
Number of configuration changes which are not documented nor approved in accordance with the requirements or procedures and number of incorrect baseline configurations noted by the licensee	**E10.3** Baseline Configuration, **E10.4** Configuration Change Control **E3.7** Integrity Verification	All CDA configuration changes which were not documented nor approved in accordance with the requirements or procedures.	Undocumented nor approved changes or incorrect changes as a numeric value explained in detail. Un-approved configuration changes would normally be captured digitally in logs and audit records of SIEMs, firewalls, and IDSs and through the use of digital integrity verification tools where possible. Some devices may only be controlled physically and integrity verification may only be possible through physical control measures. Control measures and verification, may take different forms depending on limitations. Note the trending, tracking, and periodicity requirements. See the guidance in A3.1.6, E3.7, and E10.3 Undocumented nor approved changes or incorrect changes as a numeric value explained in detail. Un-approved configuration changes would normally be	Undocumented nor approved or incorrect changes x

3 Initial Documentation Requests – RFI #1

			captured digitally in logs and audit records of SIEMs, firewalls, and IDSs and through the use of digital integrity verification tools where possible. Some devices may only be controlled physically and integrity verification may only be possible through physical control measures. Control measures and verification, may take different forms depending on limitations. For those licensee's that are reporting a quantitative value for this metric of >2, provide quantitative or qualitative context as to the health of the licensee's cyber program for this control, for example: Quantitative: 5 undocumented nor approved or incorrect changes on device configurations against the total number of audits performed during the period Or, Qualitative: A COMPLETED causal analysis addressing the	

3 Initial Documentation Requests – RFI #1

			increased number of non-compliances. If the Licensee provides the performance metric data as described here, then the Inspection Team shall determine the performance metric submission adequate.	

3 Initial Documentation Requests – RFI #1

4. Malicious Code Identification:

Perf. Metric	Security Control(s) Highlighted	Sample Size	Measurement	Count/ Numeric Data
Number of incidents where malicious code was not detected at the security boundary device entry and exit points, on CDAs, workstations, servers, and mobile computing devices at an interval commensurate with risk determination, and real-time scans of files	**E3.3** Malicious Code Protection **E3.4** Monitoring Tools and Techniques	Number of incidents where malicious code was not detected at the security boundary device entry and exit points and on CDAs (if applicable), workstations, servers, and mobile computing devices on the network	Report the total number of incidents where malicious code was not detected at the boundary, PMMD kiosks, and on CDAs (provide the analysis for not detecting the malicious code and how the malicious code was ultimately discovered, per incident, in a separate form). Record that numeric result in this form. (Malicious as defined by Webster's dictionary states; having or showing a desire to cause harm, given to, marked by, or arising from malice.) Note the trending, tracking, and periodicity requirements. See the guidance in A3.1.6, E3.3, and E3.4 If the Licensee provides the performance metric data as described here, then the Inspection Team shall determine the performance metric submission adequate.	Malicious code not detected at the security boundary and network **x**

3 Initial Documentation Requests – RFI #1

Number of scans not performed in accordance with procedures and periodicity requirements.	**E3.3** Malicious Code Protection	Number of scans of security boundary devices entry and exit points, CDAs, workstations, servers, and mobile computing devices to detect and eradicate malicious code not performed	Report the total number of scans not performed in accordance with procedures on security boundary devices, CDAs, workstations, servers, and mobile computing devices. Record that numeric result in this form. Scans for malicious code are performed digitally in logs, audit records, SIEMs, firewalls, IDSs and on other digital devices. Note the trending, tracking, and periodicity requirements. See the guidance in A3.1.6 and E3.3 If the Licensee provides the performance metric data as described here, then the Inspection Team shall determine the performance metric submission adequate.	Periodic scans not performed in accordance with procedures. **x**

3 Initial Documentation Requests – RFI #1

5. Security Functionality

Perf. Metric	Security Control(s) Highlighted	Sample Size	Measurement	Count/ Numeric Data
Number of security functions not tested	**E3.4** Monitoring Tools and Techniques, **E3.6** Security Functionality Verification	All CDAs that were *not* verified and documented, in accordance with requirements, upon startup and restart, or when anomalies are discovered.	Report the number of Cyber intrusion detection and prevention systems that were *not* tested and verified in accordance with requirements and the number of security functions of CDAs upon startup/restart not tested. Testing and verification is conducted digitally, however, some devices may only be tested and verified physically. Describe in detail the manual, non-digital or alternate method for testing and verification. Derived number must be explained in detail and represented as a numeric value or count. Record that numeric result in this form. (Security function in this context is any automated or manual function necessary to meet a cyber security control described in the licensee's requirements. The definition of restart is whenever the system's firmware, BIOS, or operating system bootstrap routine is invoked following a power on or a soft reset action.) Security function failures can be identified digitally in logs, audit records, SIEMs, PMMD kiosks, and IDSs. If the security functions are conducted through physical	CDAs not Tested: x

3 Initial Documentation Requests – RFI #1

			security controls those function failures would be identified through review and evaluation of the physical security processes, configuration management processes, work control processes, and device functionality testing processes. Note the trending, tracking, and periodicity requirements. See the guidance in A3.1.6, E3.4, and E3.6 If the Licensee provides the performance metric data as described here, then the Inspection Team shall determine the performance metric submission adequate.	

3 Initial Documentation Requests – RFI #1

6. Security Awareness and Assessment Team

Perf. Metric	Security Control(s) Highlighted	Sample Size	Measurement	Count/ Numeric Data
Personnel are provided necessary training to perform their assigned duties.	**A4.8** Cyber Security Training and Awareness **E9.2** Awareness Training **E9.3** Technical Training **E9.4** Specialized Cyber Security Training	All personnel assigned who require cyber security training	Note the trending, tracking, and periodicity requirements. See the guidance in A3.1.6, E9.2, and E9.3 If the Licensee provides the performance metric data as described here, then the Inspection Team shall determine the performance metric submission adequate.	Number of personnel who have not received cyber security training in accordance with requirements and procedures and who have performed cyber work and not been trained x
A Cyber Security Assessment Team (CSAT) is formed consisting of individuals with broad knowledge in specific areas in accordance with requirements and procedures.	**A3.1.2** Cyber Security Assessment Team	All personnel necessary to be assigned	If the Licensee provides the performance metric data as described here, then the Inspection Team shall determine the performance metric submission adequate.	Number of personnel who have not been assigned in accordance with requirements and procedures x

3 Initial Documentation Requests – RFI #1

7. System Hardening

Perf. Metric	Security Control(s) Highlighted	Sample Size	Measurement	Count/ Numeric Data
Boundary devices are configured to deny traffic, except that which are authorized. Number of unnecessary open ports and protocols for communication for firewalls discovered and removed.	**E6** Defense-In-Depth	All CDA boundary devices.	Report the total number of unnecessary open ports and protocols for communication for all boundary firewalls discovered and corrected. Derived number must be explained in detail and represented as a numeric value or count. Note the trending, tracking, and periodicity requirements. See the guidance in A3.1.6 and E6 If the Licensee provides the performance metric data as described here, then the Inspection Team shall determine the performance metric submission adequate.	Number of unnecessary open ports and protocols for communication for firewalls discovered and removed: **x**

Return to Request for Information #1

3 Initial Documentation Requests – RFI #1

17. Provide documentation describing any cyber security changes to the access authorization program since the last cyber security inspection

    a. Provide procedures and policies that document how an individual gains access to the facility to include
        1) Initial Plant access
        2) Lost badge replacement
        3) Verification for badge renewal
        4) Badge termination:
    b. Include any revisions or changes to the above documentation as a result of either SFAQ 17-04 or the Security White Paper.

Return to Request for Information #1

3 Initial Documentation Requests – RFI #1

18. For the procedures and policies provided, provide a comprehensive list that provides the procedure/policy number along with a descriptive name of the procedure/policy (if available)
    a. Looking for a comprehensive list of the procedures/policies provided that includes both a descriptive description of the procedure/policy along with it's plant number (if applicable)
    b. Optional - cross reference to which part of the inspection procedure this procedure/policy applies

Return to Request for Information #1

3 Initial Documentation Requests – RFI #1

19. Performance testing report (if applicable)

a. If the licensee has elected to perform performance testing, submit a copy of the performance test report

Return to Request for Information #1

4 Initial Documentation Requests – RFI #2

For Items 1-13 in RFI #2, these only apply to the systems that have been selected for Inspection

1. Ongoing Monitoring and Assessments performed on the system

   a. Review any ongoing monitoring or assessment that were performed on the selected systems since the last cyber security inspection.
   b. The ongoing monitoring program includes:
      - Configuration management of CDAs;
      - Cyber security impact analyses of changes to the CDAs or their environment(s) to ensure that implemented cyber security controls are performing their functions effectively;
      - Ongoing assessments to verify that the cyber security controls implemented for CDAs remain in place throughout the life cycle of the CDA;
      - Verification that rogue assets are not connected to the network infrastructure;
      - Ongoing assessments of the need for and effectiveness of the cyber security controls identified in Appendices D and E of NEI 08-09, Revision 6; and
      - Periodic cyber security program review to evaluate and improve the effectiveness of the Program.

Return to Request for Information #2

4 Initial Documentation Requests – RFI #2

2. Security Assessments for Selected Systems

   a. The licensee should provide Security assessments performed for all CDA's for the systems that have been selected for inspection.
   b. For the security assessments provided, the licensee should be able to explain how the controls provide for defense-in-depth through integration of systems, technologies, programs, equipment, supporting processes and implementing procedures to ensure the effectiveness of the program. (2.2.7)
   c. For the security assessments provided the licensee should be able to explain how these measures provide the capability to detect, delay, respond and recover from a cyber attack up to and including the design basis threat in 10 CFR 73.1 (2.2.13)

Return to Request for Information #2

4 Initial Documentation Requests – RFI #2

3. All vulnerability screening/assessments or scans performed on the selected system(s) since the last inspection

    a. Provide evidence for vulnerability scans or vulnerability assessments and the resultant reports;
    b. Provide evidence of remediation activities for vulnerabilities identified during the scan or assessment
    c. Provide a list of the most recent vulnerabilities from alerts and advisories that affect the asset
    d. Provide documentation supporting the screening and disposition of these identified vulnerabilities

Return to Request for Information #2

4 Initial Documentation Requests – RFI #2

4. Documentation for any Network-based Intrusion Detection System (NIDS/NIPS), Host-based Intrusion Detection Systems (HIDS), Security Information and Event Management (SIEM) systems and intra-security level firewalls documentation for system(s) chosen for inspection (ORFI 10, 11 and 12)

   a. For any host-based intrusion detection system (HIDS) installed as a cybersecurity countermeasure on plant CSs/CDAs in the system(s) selected for inspection provide the following:
      1) A list of CSs/CDAs and/or computers on which the HIDS has been installed;
      2) Vendor technical literature on the HIDS product;
      3) Current user-alterable HIDS-associated configuration settings within the CSs/CDAs;
      4) The test procedures used to verify HIDS functionality and effectiveness;
      5) The most recent testing results for each HIDS deployment;
      6) The list of personnel with the authority and expertise to test, maintain and administer the HIDS;
      7) The training details and personnel records for any vendor-provided product training,
      8) The list of personnel who are authorized and trained to monitor the HIDS alerts and alarms;
      9) If the HIDS is remotely monitored (e.g., at a fleet-level Security Operations Center [SOC]) provide documentation on the measures employed to ensure that remote monitoring is performed in a secure manner that does not create additional exploitable vulnerabilities;
      10) The procedures used by personnel when responding to and assessing a HIDS alert and/or alarm;
      11) The procedures for updating the HIDS to maintain and augment any “signatures” and/or rulesets used by the HIDS; and
      12) If the HIDS are integrated into a Security Information and Event Management (SIEM) system provide a description of how this is accomplished and the measures employed to ensure that SIEM integration is performed in a secure manner that does not create an attack pathway to the CSs/CDAs.

   b. For any network intrusion detection/protection system (NIDS/NIPS) installed as a cybersecurity countermeasure on the system(s) selected for inspection provide the following:
      1) List of network locations, where a “sensor” has been installed;
      2) Vendor technical literature on the NIDS/NIPS product;
      3) Technical specifications for the sensors being used including:
         i. Manufacturer
         ii. Make/Model
         iii. Firmware version
         iv. Throughput (packets/frames per second);
         v. Security capabilities of the device (i.e., information gathering, logging, detection, and prevention, respectively)

4) Current user-alterable configuration settings;
5) The NIDS/NIPS test procedures;
6) The most recent testing results, including testing of the processing/bandwidth capacity of the individual sensors and overall NIDS/NIPS as a system;
7) List of personnel with authority and expertise to test, maintain and administer the NIDS/NIPS;
8) Training details and personnel records for any vendor-provided product training;
9) List of personnel who are authorized and trained to monitor the NIDS/NIPS alerts and alarms;
10) If the NIDS/NIPS is remotely monitored (e.g., at a fleet-level SOC) provide documentation on the measures employed to ensure that remote monitoring is performed in a secure manner that does not create additional exploitable vulnerabilities;
11) Procedures used by personnel when responding to and assessing a NIDS/NIPS alert and/or alarm;
12) The procedures for updating the NIDS/NIPS to maintain and augment any "signatures" and/or rulesets used by the NIDS/NIPS;
13) Specifications on mechanisms used to provide message traffic to NIDS/NIPS sensors (e.g., Ethernet switch SPAN/mirror ports, aggregating network taps, passive taps, etc.);
14) Bandwidth/traffic analysis that shows expected message processing load for each sensor; and
15) Information on the NIDS/NIPS rules and/or signatures specifically developed to monitor and assess any industrial traffic employed by various plant systems (e.g., MODBUS®/TCP, Distributed Network Protocol (DNP3), Inter-Control Center Communications Protocol (ICCP), Process Field Net (PROFINET), EtherNet/IP, HART-IP, etc.).

c. For any SIEM and/or log collection and analysis products (e.g., a System Log (SYSLOG) server) installed as a cybersecurity countermeasure on plant networks provide the following:
1) List of computers, systems, CDAs, devices, other security mechanisms (e.g., HIDS, NIDS/NIPS, firewalls, Network Access Control (NAC), etc.) and network components (e.g., switches, routers, etc.) from which logs are reported or extracted from for analysis purposes;
2) Vendor literature on the SEIM product;
3) The specification on the types of logs and log contents reported or extracted from each of the aforementioned items listed in the prior/first bullet;
4) Technical details on the communication connectivity used to report or extract information from each of the aforementioned items listed in the first bullet;
5) Current user-alterable configuration settings for the SEIM;
6) The SEIM test procedures used to validate its functionality;
7) The most recent testing results;
8) List of personnel with the authority and expertise to test, maintain and administer the SEIM;
9) Training records for any vendor-provided product training;

4 Initial Documentation Requests – RFI #2

10) List of personnel who are authorized and trained to monitor the SEIM alerts and alarms;
11) Explain how the SIEM is monitored and alerts processed to response personnel;
12) If the SIEM is remotely monitored (e.g., at a fleet-level SOC) provide documentation on the measures employed to ensure that remote monitoring is performed in a secure manner that does not create additional exploitable vulnerabilities;
13) Procedures used by personnel when responding to and assessing a SEIM alert and/or alarm;
14) Procedures for updating SIEM to augment or enhance its analytical mechanisms for detecting new threats, malware and attack methodologies; and
15) Details on the rules and/or analysis metrics specifically developed to enable the SIEM to receive, process, and assess threats to, and attacks on safety and security CSs/CDAs.

Return to Request for Information #2

4 Initial Documentation Requests – RFI #2

5. Provide documentation for intra-security level firewalls and boundary devices used to protect the selected system(s)

   a. For any intra-security level firewall or boundary device used to protect the selected system provide the following:
      1) Vendor technical literature on the firewall or boundary device product;
      2) Copies of Firewall and/or boundary device configuration files
      3) Copies of firewall and/or boundary device log files for the last 30 days
      4) Results of functional tests performed since the last inspection on either the firewall or boundary device.
      5) Cross reference of what devices are inheriting protections from these devices
      6) Firewall or boundary device rule sets that have been implemented
      7) Documentation that shows log reviews for affected firewall and/or boundary devices were conducted as required.
      8) integration is performed in a secure manner that does not create an attack pathway to the CSs/CDAs.

Return to Request for Information #2

4 Initial Documentation Requests – RFI #2

6. Copies of all periodic reviews of the access authorization list for the selected system(s) since the last inspection

   a. Provide evidence (e.g., work orders, periodic maintenance schedules, critical group changes, etc.) of the periodic review of access authorization lists for select system(s).

Return to Request for Information #2

4 Initial Documentation Requests – RFI #2

7. Baseline configuration data sheets for the selected system(s)

   a. Provide baseline configurations for selected system;
      1) If baseline information IAW E.10.3 in not maintained in a consolidated format, provide a summary sheet of documents that contain the baseline information and marked copies of those documents referenced.
   b. Provide evidence for the last time the baseline configurations were audited

Return to Request for Information #2

4 Initial Documentation Requests – RFI #2

8. Any security impact analysis performed on the selected system(s) since the last inspection

   a. Provide documentation to describe any recent changes to the asset, e.g., Engineering Design Changes, work orders
   b. For each recent change provide a Security Impact Analysis, or justification as to why the changes are not significant enough to require one
   c. Provide procedures for Security Impact Analysis

Return to Request for Information #2

4 Initial Documentation Requests – RFI #2

9. Copies of purchase order documentation for any new equipment purchased for the selected system(s) since the last inspection

   a. Provide documentation showing chain of custody from the vendor to the site..
   b. For each purchase order, provide a Security Impact Analysis on the digital components that will be affected by the new purchase.
   c. Provide the current status of the purchase (e.g., Sitting in the warehouse, currently in a development environment).

Return to Request for Information #2

4 Initial Documentation Requests – RFI #2

10. Copy of any cyber security drills performed since the last inspection

    a. Provide a copy of any cyber security/incident response drills performed since the last cyber security inspection to include
        1) Copy of the drill scenario
        2) Any Corrective Actions generated as a result of the drill
        3) List of personnel involved with the drill

Return to Request for Information #2

4 Initial Documentation Requests – RFI #2

11. Copy of the individual recovery plan(s) for the selected system(s) including documentation of the results of the last time the backups were executed.

    a. Copy of individual recovery plans for the selected system(s) indicating how the affected equipment would be restored to operable
    b. Copy of the last time that the backups were executed
    c. Copy of any corrective actions generated as a result of attempting to restore a backup

Return to Request for Information #2

4 Initial Documentation Requests – RFI #2

12. Corrective actions taken as a result of cyber security incidents/issues to include previous NRC violations and Licensee Identified Violations (LIVs) since the last inspection.

    a. The licensee should provide a list of corrective actions since the previous NRC inspection. In this instance, corrective actions for applicable cyber related issues, including those related to vulnerability mitigation, should be tracked in a corrective action process consistent with physical security issues. The inspectors should be mindful that a recordable log review should be readily available to staff based upon guidance in RG 5.83 and NEI 15-09. The current physical security inspectors refer to this as a sample from their tickler file. In addition, inspectors should be mindful of the quality assurance applicability and how this equates to the dispositioning of corrective actions. Inspectors should assess the administrative procedures to ensure that cyber is encapsulated with the processes. References to RG 5.83, NEI 15-09, 73.55(b)(10), should have some record of a change and evaluation to add to the respective procedures. Should be encapsulated in the Cyber Event Notifications section

Return to Request for Information #2

5 Initial Documentation Requests – RFI #3

Request For Information #3 is the information to be provided to the NRC at the start of the inspection

1. Any cyber security event reports submitted in accordance with 10 CFR 73.77 since the last inspection.
   a. Provide all Cyber security Event Notifications (CSENs) submitted to the NRC Headquarters Operations Center via the Emergency Notification System (ENS) since November 3, 2015.[1]
   b. For each CSEN ensure the following information is contained within the CSEN:
      1) Indicate what systems, networks, devices and security mechanisms were, or were believed to be, involved in each event; and
      2) Documentation showing what incident response actions were taken.
      3) Refer to RG 5.83 and NEI 15-09 for supporting information

Return to Request for Information #3

[1] Title 10, *Code of Federal Regulations*, "Physical Protection of Plants and Materials," Part 73, Section 77, "Cyber security Event Notifications (10 CFR 73.77)," requires licensees subject to the provisions of 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks, to submit Cyber security Even Notifications as described in RG 5.83, "Cyber security Event Notifications," dated July 2015.

5 Initial Documentation Requests – RFI #3

2. Updated copies of corrective actions taken as a result of cyber security incidents/issues to include previous NRC violations and Licensee Identified Violations (LIVs) since the Corrective Actions for RFI #2 were submitted.
   a. The licensee should provide a list of corrective actions that were generated since the corrective actions provided for RFI #2 were submitted.
      1) Also include any corrective actions generated as a result of self assessments performed prior to the inspection and any updates to previously submitted corrective actions

Return to Request for Information #3

Appendix A – Glossary of Terms

A number of terms and words are used in this document and to ensure an alignment on the precise meaning and usage of these terms the following glossary provides the interpretation and meaning used herein.

Word/Term/Phrase	Intended Meaning/Usage
Air-gapped	See “Isolated”
COTS	“COTS” means commercial off the-shelf devices or software (i.e., shipped and received with normal and expected commercial vendor shipping/packaging such as shrink-wrap, tamper seal or other recognizable packaging and marking) that is available from multiple sources developed to run unmodified as delivered by the original developer. This would include such products as commercially available OSs (e.g., MS Windows, Linux, O SX, TXS, etc.), general purpose application software (i.e., MS Office, Corel, Open Office, Structured Query Language (SQL) Server, etc.), and Open-Source products, where “builds” can be verified and are obtained from known trusted sources. Firmware such as Basic Input/output System (BIOS) updates, field upgradable commercial sensors (i.e., Pressure Transmitters, Flow Sensors, Level Sensors, etc.), and other off the shelf firmware upgradable hardware (i.e., Hard Drives, Video Cards, Digital Versatile Disc (DVD) Drives, Embedded OS, etc.) would be considered COTS.
DCS	“DCS” Distributed Control System, is a computerized control system for a process or plant, which combines the following into a single automated system: human machine interface (HMI), logic solvers, data acquisitions components, historian, common database, alarm/event management, and a common engineering suite. DCSs follow very specific design requirements and contain all the elements noted above. A systems of distributed data acquisition components would not be considered a DCS.
Fieldbus	“Fieldbus” is a specialized LAN used to provide intercommunications among smart instruments and control elements for data acquisition and process control purposes. A fieldbus can be based on Ethernet technology (e.g., PROFINET) or on a less complex serial communications technology better suited for hazardous areas and designed to provide device power (e.g., Foundation Fieldbus H1 or PROFIBUS) or it can be based on wireless communication technology (e.g., WirelessHART or ISA 1100.11a).
HIDS	“Host-Based Intrusion Detection System” is a technology generally consisting of software installed onto one or more computers to detect abnormal, suspicious and/or malicious activity in those computers using various means of detection, plus a central console that collects, correlates and analyzes information from the participating computers to determine if an alert should be generated.

Appendix A – Glossary of Terms

Word/Term/Phrase	Intended Meaning/Usage
Isolated	"Isolated" means an individual device/CDA that has no form of digital communication interconnectivity, either wired or wireless, including LAN and WAN connectivity as well as point-to-point/multi-point serial connectivity. This segregation could be either due to the absence of communication interfaces (hardware and/or software) or due to the existing interfaces having been disabled physically, electrically, or administratively.
Isolated LAN	"Isolated LAN" is a wired (not wireless) local area network physically constrained to a specified geographic area, having no gateways or bridges that provide information/message exchanges with any other network, and used to interconnect a defined and specific set of devices/elements to perform/support a specified set of functions
LAN	"Local Area Network" is a network that covers a smaller geographic area (e.g., an industrial facility) and thus can be implemented using communications technologies that have a shorter range such as "Ethernet".
NIDS/NIPS	"Network-Based Intrusion Detection System" is a technology generally consisting of one or more specialized computers (called "sensors") used to monitor and process network message traffic between and among network-connected computers to detect abnormal, suspicious and/or malicious activity using various means of detection, plus a central console that collects, correlates and analyzes information from the sensors in order to determine if an alert should be generated.
SIEM	"Security Information and Event Management" is an information collection and analysis technology that uses logs and other types of information collected from computers, security devices (e.g., firewalls), network components (e.g., routers and switches) and other cyber detective systems (e.g., NIDS/NIPS and HIDS) to attempt to detect and identify abnormal, suspicious and/or malicious activity using a range of analytical methods.
WAN	"Wide-Area Network" is a network that covers a large geographic area (e.g., a country) and thus requires the use of telecommunication infrastructure suitable for long distance data transmission such as FDDI, ATM and SONET technologies. WANs may also incorporate an over greater number of member nodes than would be typical for a LAN. The largest example of a WAN is the INTERNET.
WLAN	"Wireless LAN" is a LAN that makes use of radio-based communications technologies (e.g., Wi-Fi or Worldwide Interoperability for Microwave Access (WiMAX)) to interconnect the member nodes. A subset or variation of this are the PICONET and the personal area network (PAN) which use short-range radio technologies (e.g., Bluetooth) and thus are more distance/coverage-area limited.

Appendix A – Glossary of Terms

Return to Table of Contents

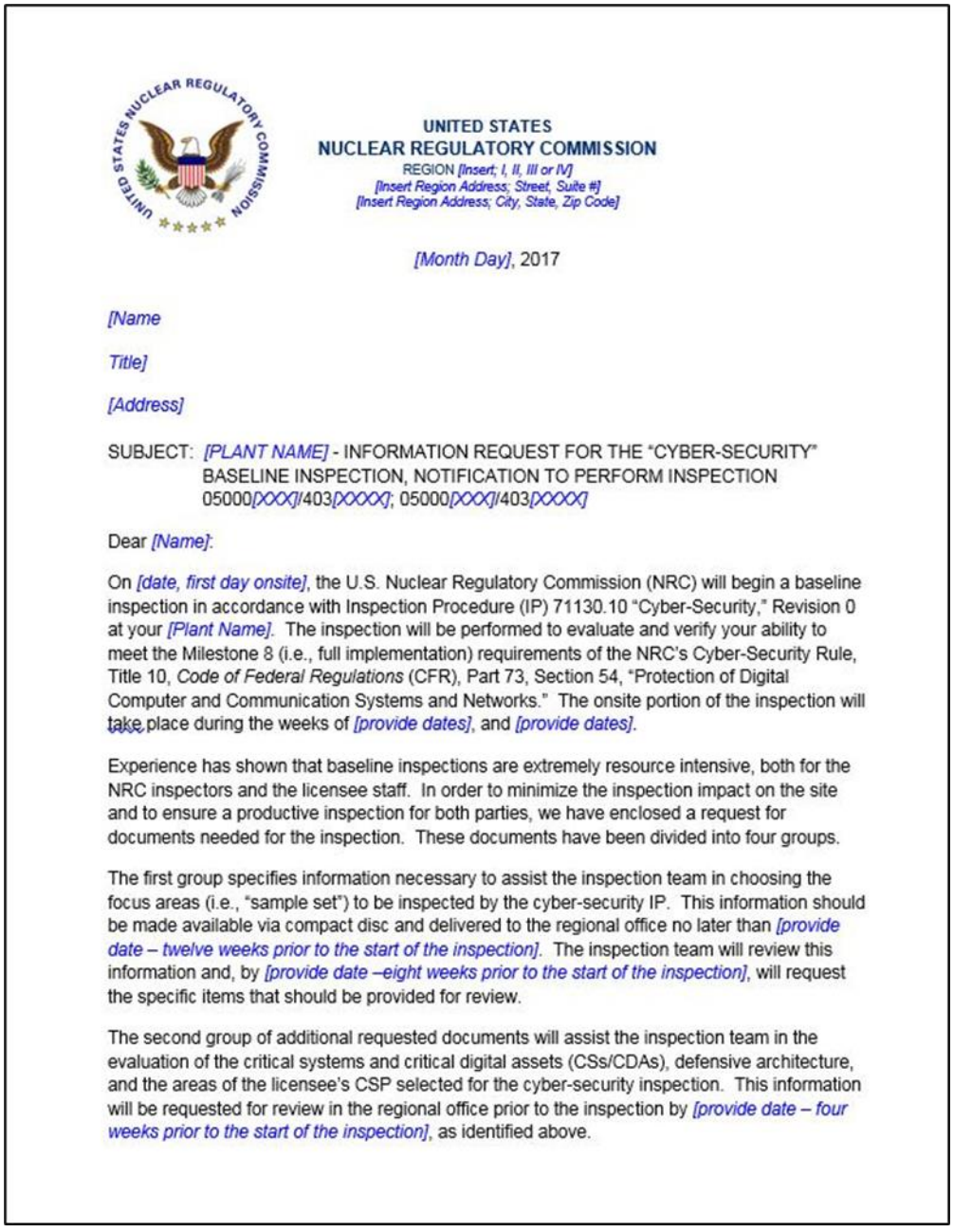
Appendix B – Transmittal Letter (Example)

The following transmittal letter template should be used as the RFI and notification letter to the licensee. The letter should be sent at least 120 days prior to the start date of the cyber security inspection. To obtain the complete MS Word template, double click on the MS Word icon.

Return to Table of Contents

Cyber-Security RFI and Notification Ltr

Appendix B – Transmittal Letter (Example)



UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION *[Insert; I, II, III or IV]*
[Insert Region Address; Street, Suite #]
[Insert Region Address; City, State, Zip Code]

[Month Day], 2017

[Name

Title]

[Address]

SUBJECT: *[PLANT NAME]* - INFORMATION REQUEST FOR THE "CYBER-SECURITY" BASELINE INSPECTION, NOTIFICATION TO PERFORM INSPECTION 05000*[XXX]*/403*[XXXX]*; 05000*[XXX]*/403*[XXXX]*

Dear *[Name]*:

On *[date, first day onsite]*, the U.S. Nuclear Regulatory Commission (NRC) will begin a baseline inspection in accordance with Inspection Procedure (IP) 71130.10 "Cyber-Security," Revision 0 at your *[Plant Name]*. The inspection will be performed to evaluate and verify your ability to meet the Milestone 8 (i.e., full implementation) requirements of the NRC's Cyber-Security Rule, Title 10, *Code of Federal Regulations* (CFR), Part 73, Section 54, "Protection of Digital Computer and Communication Systems and Networks." The onsite portion of the inspection will take place during the weeks of *[provide dates]*, and *[provide dates]*.

Experience has shown that baseline inspections are extremely resource intensive, both for the NRC inspectors and the licensee staff. In order to minimize the inspection impact on the site and to ensure a productive inspection for both parties, we have enclosed a request for documents needed for the inspection. These documents have been divided into four groups.

The first group specifies information necessary to assist the inspection team in choosing the focus areas (i.e., "sample set") to be inspected by the cyber-security IP. This information should be made available via compact disc and delivered to the regional office no later than *[provide date – twelve weeks prior to the start of the inspection]*. The inspection team will review this information and, by *[provide date –eight weeks prior to the start of the inspection]*, will request the specific items that should be provided for review.

The second group of additional requested documents will assist the inspection team in the evaluation of the critical systems and critical digital assets (CSs/CDAs), defensive architecture, and the areas of the licensee's CSP selected for the cyber-security inspection. This information will be requested for review in the regional office prior to the inspection by *[provide date – four weeks prior to the start of the inspection]*, as identified above.

Appendix C – List of Acronyms

LIST OF ACRONYMS

ACL	Access Control List
AP	Access Point
ASCII	American Standard Code for Information Interchange
ATM	Asynchronous Transfer Mode
AV	Anti-Virus
BIOS	Basic Input/output System
BOP	Balance-of-Plant
CCB	Configuration Control Board
CDA	Critical Digital Asset
CFR	Code of Federal Regulations
COTS	Commercial Off-The-Shelf
CS	Critical System
CSAT	Cyber security Assessment Team
CSEN	Cyber security Event Notification
CSIRT	Cyber security Incident Response Team
CSP	Cyber security Plan
CSV	Comma Separated Values
DCS	Distributed Control System
DEC	Digital Equipment Corporation
DNP	Distributed Network Protocol
DVD	Digital Versatile Disc
EIN	Equipment ID Number
EP	Emergency Preparedness
EPN	Equipment Part Number
FDDI	Fiber Distributed Data Interface
HART	Highway Addressable Remote Transducer
HIDS	Host-based intrusion Detection Systems
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
I/O	Input/output
ICCP	Inter-Control Center Communications Protocol
IP	Inspection Procedure
IPX/SPX	Internetwork Packet Exchange/Sequenced Packet Exchange
IRIG-B	Inter-Range Instrumentation Group Time Code B
ISA	International Society for Automation (
LAN	Local Area Network
M&TE	Measurement and Test Equipment
MAC	Media Access Control
MD	Mobile Device
NAC	Network Access Control
NAS	Network-Attached Storage

Appendix C – List of Acronyms

NEI	Nuclear Energy Institute
NET	Network
NIDS/NIPS	Network Intrusion Detection System/Network Intrusion Prevention System
NRC	U.S. Nuclear Regulatory Commission
O&M	Operational and Management
OS	Operating System
PBX	Private Branch Exchange
PLC	Programmable Logic Controller
PM	Portable Media
PROFIBUS	Process Field Bus
PROFINET	Process Field Net
RFI	Request for Information
RG	Regulatory Guide
Rlogin	Remote Login
SCADA	Supervisory Control and Data Acquisition
SCM	Software Configuration Management
SDH	Synchronous Digital Hierarchy
SDLC	Software Development Life Cycle
SIEM	Security Information And Event Management
SGI	Safeguards Information
SNA	Systems Network Architecture
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
SONET	Synchronous Optical Networking
SPM	Software Patch Management
SQA	Software Quality Assurance
SQL	Structured Query Language
SSEP	Safety, Security, and Emergency Preparedness
SSH	Secure Shell
SYSLOG	System Log
TCP/IP	Transmission Control Protocol/Internet Protocol
USB	Universal Serial Bus
V&V	Verification and Validation
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WAN	Wide-Area Network
WiMAX	Worldwide Interoperability for Microwave Access
XML	Extensible Markup Language

Return to Table of Contents