Generic RAI Proposed Resolution – Security Control RAIs

NRC Comment / RAI	NEI Response/Considerations	NEI 08-09 Proposed Changes (if any)
Open Issue One: Defensive Strategy	This response supersedes the response to Draft RAI 7 provided on 3/5/2010 and 3/26/2010. The bracketed text is revised to provide additional guidance on the level of detail to be provided in the Defensive Strategy.	Revise NEI 08-09, Revision 3, Section 4.3 as follows: Replace the content of Section 4.3 with the following: "4.3 DEFENSE-IN-DEPTH PROTECTIVE STRATEGIES 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. The defensive strategy describes the defensive security architecture, identifies the protective controls associated within each security level, implements cyber security controls in accordance with Section 3.1 of this Plan, employs the Defense-in-Depth measures described in NEI 08-09, Appendix E, Section 6, and maintains the cyber security program in accordance with in Section 4 of this Plan. The defensive architecture has been implemented, documented, and is maintained to protect CDAs that have similar cyber risks from other CDAs, systems or equipment by establishing the logical and physical boundaries to control the data transfer between

		boundaries. This defensive architecture provides for cyber security defensive levels separated by security boundaries devices, such as firewalls and diodes, at which digital communications are monitored and restricted. Systems requiring increasing degrees of security are located within an increasing number and strength of boundaries. The criteria below are utilized in the defensive architecture. [Insert site-specific Defensive Architecture description that answers the following three questions: 1. In what level or levels are safety and security CDAs located? 2. What are the boundaries, and what are the data flow rules between defensive levels? 3. How are the data flow rules enforced? For example, if a deterministic boundary device is used, the description can be brief (e.g. data flow is enforced between levels 3 and 4 using a data diode). However, if a non-deterministic boundary device is used (e.g., a firewall), the plan needs to include the criteria that the device will apply to enforce the data flow rule (e.g., Section 6 of NEI 08-09, Revision 3, Appendix E non-deterministic data flow criteria).

		Two hypothetical examples are provided below to illustrate the level of detail sufficient for this section. Example 1: The site defensive model implements all of the following: • The defensive model consists of 4 layers, with layer 4 having the greatest level of protection. • Safety CDAs are in Level 4. • Security CDAs are in Level 4, 3. • The boundary between Level 3 and Level 2 is implemented by one or more deterministic devices (i.e., data diodes, air gaps) that isolate CDAs in or above Level 3. • Data flows between Levels are restricted through the use of cyber security boundary control devices. • Cyber security boundary control devices implement cyber security controls in accordance with Section 3.1.6 of this Plan. Example 2: The site defensive model implements all of the following: • The defensive model consists of 4 layers, with layer 4 having the greatest level of protection. • Safety CDAs are in Level(s) 4. • Security CDAs are in Level(s) 4, and 3.

		• CDAs within a particular security level may not share a common network. • Safety CDAs are isolated from all other CDAs through the use of deterministic boundary devices (i.e., data diodes, air-gaps). • Security CDAs are isolated from all other CDAs by a defensive boundary that implement the rule set characteristics for non-deterministic information flow enforcement described in the Defense-In-Depth cyber security control in NEI 08-09, Revision 3, Appendix E, Section 6. • Information flows between Security CDAs in one level and Security CDAs in another level are restricted through the use of a firewall and network-based intrusion detection system. The firewall implements the Information Flow Enforcement cyber security control in NEI 08-09, Revision 3, Appendix D, Section 1.4.] For this defensive architecture to be effective in protecting CDAs from cyber attacks the above characteristics are consistently applied, along with the technical, management, and operational security controls discussed in Appendices D and E of NEI 08-09, Revision 6. The cyber security defensive model is enhanced by physical and administrative cyber security controls implemented by the Physical

		Security Program. Physical barriers such as locked doors, locked cabinets, and/or locating CDAs in the protected area or vital area are also used to mitigate risk."
Open Issue 3: Storage of records	This response supersedes the response to Draft RAI 28 provided on 3/5/2010 and 3/26/2010. The section will be revised to clarify the records retention duration for logs. CDAs may be non-networked, or due to minimal system resources, will not be able to retain logs for lengthy durations. Accordingly, the ability to implement logging capabilities must be tailored in accordance with Section 3.1.6.	Revise NEI 08-09, Revision 3, Appendix A, Section 4.13 read as follows: 4.13 DOCUMENT CONTROL AND RECORDS RETENTION AND HANDLING [Licensee/Applicant] has established the necessary measures and governing procedures to ensure that sufficient records of items and activities affecting cyber security are developed, reviewed, approved, issued, used, and revised to reflect completed work. The following will be retained as a record until the Commission terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified by the Commission: • Records of the assessment described in Section 3.1 of this Plan; • Records that are generated in the Establishment, Implementation, and Maintenance of the Cyber Security Program; • Records of Addition and Modification of Digital Assets; and • Records and supporting technical documentation required to satisfy the

		requirements of the Rule CDA audit data will be retained for no less than 12 months. CDA auditing capabilities are configured in accordance with Section 3.1.6 of this plan. Where a central logging server is employed, the audit data received will be retained for no less than 12 months. The following audit data will be retained: • Audit data described in Appendix D, 2.3, "Content of audit records" • Audit data that support Appendix E, "Defense-in-Depth" security control will be retained to provide support for after-the-fact investigations of security incidents and satisfy the requirements of 10 CFR 73.54 and 10 CFR 73.55. Audit (digital and non-digital) data include: o Operating system logs o Service and application logs o Network device logs For the purposes of this Plan, audit data is not required to be maintained under the QA Records Program. Individual Cyber Security Training Records will be documented and maintained for 3 Years.
36. 10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risks. The	This response supersedes the response to Draft RAI 36 proposed	Clarifications and changes to the specific security controls referenced in this RAI are

[SITE/LICENSEE] Cyber Security Plan (CSP) describes in multiple sections that the licensee will perform a "risk assessment." For example, Appendix D, Section 1.3 states: "Authorizes personnel access to privileged functions and security-relevant information consistent with the risk assessment established policies and procedures." However, the [SITE/LICENSEE] CSP does not describe what this risk assessment is, how it is performed, or how the results are used. This term is used throughout the CSP including: Appendix D – 1.1 Appendix D – 1.2 Appendix D – 1.3 Appendix D – 1.7, Appendix D – 1.10 Appendix D – 1.17 Appendix D – 1.18 Appendix D – 2.2 Appendix D – 2.5 Appendix D – 2.6 Appendix D – 2.8, Appendix D – 2.9, Appendix D – 3.7 Appendix D – 3.15 Appendix D – 4.1 Appendix D – 4.3 Appendix D – 5.2 Appendix E – 1.5, Appendix E – 1.6	on 3/26/2010. Clarifications and changes to the specific security controls referenced in this RAI are provided in the supplemental table, below.	provided in the supplemental table, below. Revise NEI 08-09, Revision 3, Section 3.1.6 to amend Step 2. The three-step process in NEI 08-09, Section 3.1.6 would then read: 1) Implementing the cyber security controls in Appendices D and E of NEI 08-09, Revision 3. 2) Implementing alternative controls/countermeasures that eliminate threat/attack vector(s) associated with one or more of the cyber security controls enumerated in (1) above by: a) Documenting the basis for employing alternative countermeasures; b) Performing and documenting the analyses of the CDA and alternative countermeasures to confirm that the countermeasures provide the same or greater cyber security protection as the corresponding cyber security control; and c) Implementing alternative countermeasures that provide at least the same degree of cyber security protection as the corresponding cyber security control; or d) Implementing an alternative frequency or periodicity for the security control employed by documenting the basis for the alternate frequency or periodicity. The basis incorporates one or more of

Appendix E – 3.4 Appendix E – 5.5 Appendix E – 5.10, Appendix E – 6 Appendix E – 7.3, Appendix E – 8.2 Appendix E – 8.3, Appendix E – 8.5, Appendix E – 9.4 Appendix E – 10.3 Appendix E – 10.5 Appendix E – 10.6 Appendix E – 10.8 Appendix E – 11.2 Appendix E – 11.4, How is the risk assessment performed and how are the results used?		the following: i) NRC Regulations, Orders ii) Operating License Requirements (e.g., Technical Specifications) iii) Site operating history iv) Industry operating experience v) Experience with security control vi) Guidance in generally accepted standards (e.g., NIST, IEEE, ISO) vii) Audits and Assessments viii) Benchmarking ix) Availability of new technologies 3) Not implementing one or more of the cyber security controls by performing an analyses of the specific cyber security controls for the CDA that will not be implemented to provide a documented justification demonstrating the attack vector does not exist (i.e., not applicable) and therefore those specific cyber security controls are not necessary. Revise NEI 08-09, Revision 3, Appendix A, Section 4.2 to add the following paragraph to the end of the Section: Many security controls have actions that are required to be performed on specific frequencies. The frequency of a security control is met if the action is performed within 1.25 times the frequency specified in the control, as applied, and as measured from the previous performance of the action. This extension facilitates scheduling

		and considers plant operating conditions that may not be suitable for conducting the security control action (e.g., transient conditions, other ongoing surveillance or maintenance activities). These provisions are not intended to be used repeatedly merely as an operational convenience to extend frequencies beyond those specified.
	RAI 36 Supplemental Table	**Green highlight text is the new text. Red highlight text will be stricken.**
Security Control	**NEI Response/Considerations**	**NEI 08-09, Revision 3 – Proposed Language**
Appendix D – 1.1	A change to NEI 08-09 has been identified to address this concern.	The access control policy addresses: • Auditing of CDAs every 12 months, or upon changes in critical group personnel or major changes in system configurations or functionality; and
Appendix D – 1.2	A change to NEI 08-09 has been identified to address this concern.	**1.2 Account Management** This Technical cyber security control: • Employs computerized mechanisms that support CDA account management functions. The CDA will automatically: • Terminate temporary, guest, and emergency accounts within 31 days.
Appendix D – 1.3	A change to NEI 08-09 has been	**1.3 Access Enforcement**

	identified to address this concern.	This Technical cyber security control: • Authorizes personnel access to privileged functions and security-relevant information consistent with ~~the risk assessment~~ established policies and procedures. • Requires dual authorization for critical privileged functions and to create any privileged access for users ~~as determined by the risk assessment~~
Appendix D – 1.7	A change to NEI 08-09 has been identified to address this concern.	**1.7 Unsuccessful Login Attempts** This Technical cyber security control: • Implements security controls to limit the number of invalid access attempts by a user ~~within a maximum interval as identified in the risk assessment~~ and documented this requirement in the access control policy.
Appendix D – 1.10	A change to NEI 08-09 has been identified to address this concern.	**1.10 Session Lock** CDAs are configured to: • Initiate a session lock within 30 minutes of inactivity.
Appendix D – 1.17	A change to NEI 08-09 has been identified to address this concern.	**1.17 Wireless Access Restrictions** This Technical cyber security control • Documents, justifies, authorizes, monitors, and controls wireless access to CDAs and ensures that the wireless access restrictions are consistent with defensive strategies and defensive model and articulated in the Cyber Security Plan.

Appendix D – 1.18	A change to NEI 08-09 has been identified to address this concern. The existing 50.59 plant modification process requires an annual self-assessment to ensure no unauthorized changes are introduced. This control should maintain alignment. The IMP and the 73.55 requirements for safety-security interface further mitigate the risk of introduction of rogue connections. Yearly is reasonable for high assurance of adequate protection.	**Insecure And Rogue Connections** This Technical Cyber Security Control performs verification during deployment of CDAs, when changes or modifications occur to CDAs, and every 12 months, that CDAs are free of insecure (e.g., rogue) connections such as vendor connections and modems.
Appendix D – 2.2	A change to NEI 08-09 has been identified to address this concern.	**2.2 Auditable Events** This Technical cyber security control: • Determines and documents ~~based upon a risk assessment~~ in conjunction with safety, security and emergency preparedness functions, which CDA related events require auditing,
Appendix D – 2.5	A change to NEI 08-09 has been identified to address this concern.	**2.5 Response To Audit Processing Failures** This Technical cyber security control: • If audit processing capabilities fail for a CDA or security boundary device, the following occurs ~~based on the risk assessment:~~
Appendix D – 2.6	A change to NEI 08-09 has been identified to address this concern.	**2.6 Audit Review, Analysis, And Reporting** This Technical cyber security control:

	Activity will be performed on a quarterly basis as part of existing quarterly system engineering activities.	• Reviews and analyzes the CDAs audit records every 92 days, for indications of inappropriate or unusual activity, and reports the findings to the designated official.
Appendix D – 2.8	A change to NEI 08-09 has been identified to address this concern.	**2.8 Time Stamps** This Technical cyber security control ensures CDAs use internal system clocks to generate time stamps for audit records ~~as identified by the CDA risk assessment~~
Appendix D – 2.9	A change to NEI 08-09 has been identified to address this concern.	**2.9 Protection Of Audit Information** This Technical cyber security control • Ensures that audit information is protected at the same level as the device sources ~~as identified by risk assessment~~.
Appendix D – 3.7	A change to NEI 08-09 has been identified to address this concern.	**3.7 Transmission Confidentiality** This Technical cyber security control: • Configures the CDAs to protect the confidentiality of transmitted information ~~as determined in the risk assessment~~.
Appendix D – 3.15	A change to NEI 08-09 has been identified to address this concern.	**3.15 Secure Name / Address Resolution Service (Recursive Or Caching Resolver)** This Technical cyber security control: • Configures the systems that serve name/address resolution service for CDAs to perform data origin authentication and data integrity verification on the resolution response they receive from authoritative

		sources ~~when requested by CDAs as identified by the risk assessment~~.
Appendix D – 4.1	A change to NEI 08-09 has been identified to address this concern. Inactivity is a poor measure, as many systems are very infrequently used. When no longer needed is more appropriate, and can be tied to management controls.	**4.1 Identification And Authentication Policies And Procedures** The identification and authentication policy and procedures provide guidance on managing both user identifiers and CDA authenticators. These items include: • ~~Disabling user identifier after a maximum of 31 days of inactivity,~~ • Disabling user identifier within 31 days after the identifier is not longer needed,
Appendix D – 4.3	A change to NEI 08-09 has been identified to address this concern.	**4.3 Password Requirements** This Technical cyber security control ensures that when used, passwords meet the following requirements: • Passwords are changed every 92 days.
Appendix D – 5.2	A change to NEI 08-09 has been identified to address this concern.	**5.2Host Intrusion Detection System (Hids)** This Technical cyber security control establishes, implements, and documents requirements to: Perform rules updates and patches to the HIDS as security issues are identified to maintain the established level of system security ~~within the periodicity identified by the risk assessment~~
Appendix E – 1.5	A change to NEI 08-09 has been identified to address this concern.	**1.5 MEDIA TRANSPORT** CDA media in transport is physically protected, transported and stored to a level

		commensurate with the security classification of the data:
Appendix E – 1.6	A change to NEI 08-09 has been identified to address this concern.	**1.6 MEDIA SANITATION AND DISPOSAL** CDA media, both digital and non-digital, are sanitized prior to disposal or release for reuse ~~to a level commensurate with risk assessment determination of the sensitivity of the data:~~
Appendix E – 3.4	A change to NEI 08-09 has been identified to address this concern.	**3.4 Monitoring Tools and Techniques** This security control consists of: Competent cyber security personnel randomly test and document cyber security intrusion monitoring tools.
Appendix E – 5.5	A change to NEI 08-09 has been identified to address this concern.	**5.5 PHYSICAL ACCESS CONTROL** This security control consists of: Controlling physical access to the CDAs independent of the physical access controls for the facility ~~as required by the risk assessment~~.
Appendix E – 5.10	A change to NEI 08-09 has been identified to address this concern.	Strike NEI 08-09, Revision 3, Appendix E, Control 5.1- from NEI 08-09, this item is not in RG 5.71.
Appendix E – 6	A change to NEI 08-09 has been identified to address this concern.	**6 DEFENSE-IN-DEPTH** This security control implements and documents a defensive strategy where: • Except in the case of data diodes, contain a rule set that at a minimum,: o Are updated every 92 days;
Appendix E – 7.3	A change to NEI 08-09 has been	**7.3 INCIDENT RESPONSE TESTING AND**

	identified to address this concern.	**DRILLS** This security control consists of: Testing and conducting drills of the incident response capability for CDAs every 12 months.
Appendix E – 8.2	A change to NEI 08-09 has been identified to address this concern.	**8.2 CONTINGENCY PLAN TESTING** This security control consists of: Using scheduled and unscheduled system maintenance activities, including responding to CDA component and system failures, as an opportunity to test or exercise the contingency plan ~~consistent with the risk assessment~~.
Appendix E – 8.3	A change to NEI 08-09 has been identified to address this concern.	**8.3 CONTINGENCY TRAINING** This security control consists of: • Training personnel in their contingency roles and responsibilities with respect to the CDAs and provides refresher training every 12 months, or consistent with the existing contingency program, whichever period is shorter.
Appendix E – 8.5	A change to NEI 08-09 has been identified to address this concern.	**8.5 CDA BACKUPS** This security control consists of: • Conducting backups of user-level and system-level information. • Backing up CDAs at an interval identified for the CDA.
Appendix E – 9.4	A change to NEI 08-09 has been identified to address this concern.	**9.4 SPECIALIZED CYBER SECURITY TRAINING** Requirements for advanced training are established, implemented and documented for

		individuals who are designated security experts or specialists, including the cyber security specialists with roles and responsibilities for cyber security ~~risk assessments~~, incident response, and the execution and management of defense-in-depth protective strategies
Appendix E – 10.3	A change to NEI 08-09 has been identified to address this concern. Licensee design and configuration management programs provide extensive oversight in this area. Plant changes are too rigorous to warrant a more frequent review. Every 2 years is consistent with high assurance of adequate protection.	**10.3 BASELINE CONFIGURATION** … The up-to-date baseline configurations are documented and the configurations are audited every 24 months.
Appendix E – 10.5	A change to NEI 08-09 has been identified to address this concern.	**10.5 SECURITY IMPACT ANALYSIS** A security impact analysis is performed prior to making changes to CDAs consistent with the ~~risk assessment~~ process described in the Cyber Security Plan to manage the cyber risk resulting from the changes.
Appendix E – 10.6	A change to NEI 08-09 has been identified to address this concern.	**10.6 ACCESS RESTRICTIONS FOR CHANGE** The security control: Defines, documents, approves, and enforces physical and logical access restrictions associated with changes to CDAs and generates, retains, and audits the record every 92 days, and when there are indications that unauthorized changes may have occurred.
Appendix E – 10.8	A change to NEI 08-09 has been	**10.8 LEAST FUNCTIONALITY**

	identified to address this concern. Licensee design and configuration management programs provide extensive oversight in this area. Plant changes are too rigorous to warrant a more frequent review. Every 2 years is consistent with high assurance of adequate protection.	CDAs are reviewed every 24 months to identify and eliminate unnecessary functions, ports, protocols, and services.
Appendix E – 11.2	N/A	**N/A** – This paragraph was removed in response to RAI 69.
Appendix E – 11.4	A change to NEI 08-09 has been identified to address this concern.	**11.4 Integration of Security Capabilities** This security control documents and implements a program to ensure that new acquisitions incorporate security controls ~~consistent with the risk assessments describe in the Cyber Security Plan selected~~ based on the following:
	END **RAI 36 Supplemental Table**	
NRC Comment / RAI	**NEI Response/Considerations**	**NEI 08-09 Proposed Changes (if any)**
37. 10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risks. The [SITE/LICENSEE] Cyber Security Plan (CSP) describes in multiple sections actions that occur "periodically." For example in Appendix E, Section 3.6 of NEI 08-09, Revision 3 the CSP states: "The correct operation of security	The response is similar to the response to RAI 36. Note that reviews are performed in accordance with 10 CFR 73.55(m). The supplement table below identifies the changes to NEI 08-09, Revision 3, to address this RAI.	

functions of CDAs are verified and documented, **periodically**, upon startup and restart, upon command by a user with appropriate privilege, and when anomalies are discovered, where possible." However, the CSP does not provide the time spans for these "periods" nor does it describe how a risk assessment would produce these time spans. The same language is also used in other sections including: Section 3.1 Appendix D – 1.1 Appendix D – 2 Appendix D – 3.1 Appendix D – 4.1 Appendix D – 4.7 Appendix E – 1.1 Appendix E – 3.1 Appendix E – 4.1 Appendix E – 5.1 Appendix E – 7.1 Appendix E – 10.2 Appendix E – 11.1 Specify the time spans for these "periods" stated. If the periodicity is not consistent with the periodicity described in NEI 03-12, describe the process by which the periodicities are determined.		
	RAI 37 Supplemental Table	

	Blue highlight text is the modified text	Green highlight text is the new text. Red highlight text will be stricken.
Security Control	**NEI Response/Considerations**	**NEI 08-09, Revision 3 – Proposed Language**
Section 3.1 – Section 3.1.1	A change to NEI 08-09 has been identified to address this concern.	**3.1.1 Cyber Security Assessment and Authorization** [Site/Licensee] develops, disseminates, and periodically reviews in accordance with 10 CFR 73.55(m), and updates:
Appendix D – 1.1	A change to NEI 08-09 has been identified to address this concern.	**1.1 Access Control Policy And Procedures** A formal, documented, critical digital asset (CDA) access control policy is developed, disseminated, and reviewed in accordance with 10 CFR 73.55(m), and updated.
Appendix D – 2	A change to NEI 08-09 has been identified to address this concern.	**2.1 Audit And Accountability Policy And Procedures** This Technical cyber security control develops, disseminates, and periodically reviews in accordance with 10 CFR 73.55(m), and updated:
Appendix D – 3.1	A change to NEI 08-09 has been identified to address this concern.	**3.1 CDA, System And Communications Protection Policy And Procedures** This Technical cyber security control ensures development, dissemination, periodic review in accordance with 10 CFR 73.55(m), and updating: NOTE: This is the same as RAI 51.
Appendix D – 4.1	A change to NEI 08-09 has been	**4.1 Identification And Authentication**

	identified to address this concern.	**Policies And Procedures** This Technical cyber security control develops, disseminates, reviews, in accordance with 10 CFR 73.55(m), and updates:
Appendix D – 4.7	A change to NEI 08-09 has been identified to address this concern.	**4.7Authenticator Management** This Technical cyber security control manages CDA authenticators by performing the following: Changing/refreshing authenticators every 12 months.
Appendix E – 1.1	A change to NEI 08-09 has been identified to address this concern.	**1.1 MEDIA PROTECTION POLICY AND PROCEDURES (SGI, NON-SGI AND 2.390)** This security control develops, disseminates, reviews in accordance with 10 CFR 73.55(m), and updates:
Appendix E – 3.1	A change to NEI 08-09 has been identified to address this concern.	**3.1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES** This security control develops, disseminates, and reviews in accordance with 10 CFR 73.55(m), and updates a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among entities, and compliance.
Appendix E – 4.1	A change to NEI 08-09 has been identified to address this concern.	**4.1 SYSTEM MAINTENANCE POLICY AND PROCEDURES** This security control develops, disseminates, and reviews in accordance with 10 CFR 73.55(m), and updates:

Appendix E – 5.1	A change to NEI 08-09 has been identified to address this concern.	**5.1 PHYSICAL AND OPERATIONAL ENVIRONMENT PROTECTION POLICIES AND PROCEDURES** For those CDAs located outside of the protected area, develop, implement, review in accordance with 10 CFR 73.55(m), and update:
Appendix E – 7.1	A change to NEI 08-09 has been identified to address this concern.	**7.1 INCIDENT RESPONSE POLICY AND PROCEDURES** The security control develops, disseminates, reviews in accordance with 10 CFR 73.55(m), and updates:
Appendix E – 10.2	A change to NEI 08-09 has been identified to address this concern.	**10.2 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES** This security control develops, disseminates, reviews in accordance with 10 CFR 73.55(m), and updates a formal, documented, configuration management policy, and implementing procedures that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among entities as warranted, associated configuration management controls, and compliance.
Appendix E – 11.1	A change to NEI 08-09 has been identified to address this concern.	**11.1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES** This security control develops, disseminates, reviews in accordance with 10 CFR 73.55(m), and updates:
	END **RAI 37 Supplemental Table**	

NRC Comment / RAI	NEI Response/Considerations	NEI 08-09 Proposed Changes (if any)
38. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix D, Section 1.2, "Account Management," of the [SITE/LICENSEE] Cyber Security Plan (CSP) states: "[SITE/LICENSEE] reviews critical digital asset accounts consistent with the access control list provided in the design control package, access control program, cyber security procedures and initiates required actions on critical digital asset accounts within a maximum time period as determined by the risk assessment." The purpose of reviewing accounts frequently is to eliminate unnecessary accounts, such as temporary, guest, default, and shared accounts. This minimizes the opportunity for an adversary to exploit such accounts. A review period for physical access is in 10 CFR 73.56(j), "Access to Vital Areas." It requires licensees to update and re-approve vital area access lists at least every 31 days. Describe how the frequency selection will provide the same level of protection as the frequency currently required by 10 CFR 73.56.	A change to NEI 08-09 has been identified to address this concern. Baseline configuration disables unnecessary accounts. Comparing physical and electronic access is an inappropriate comparison. Configuration management and design mod processes support risk mitigation of this threat. Quarterly is appropriate. Quarterly is consistent with high assurance of adequate protection.	Revise NEI 08-09, Revision 3, Appendix D, Section 1.2, "Account Management," as follows: 1.2 Account Management This Technical cyber security control: • Reviews CDA accounts consistent with the access control list provided in the design control package, access control program, cyber security procedures and initiates required actions on CDA accounts at least every 92 days.

39. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. The [SITE/LICENSEE] Cyber Security Plan, Appendix D, Section 1.2, "Account Management," does not provide criteria for ensuring that the principle of "least privilege" is applied to critical digital asset (CDA) accounts. Least privilege minimizes the potential for user abuse or misuse of his/her privileges to adversely impact CDAs or safety, security, or emergency preparedness (SSEP) functions. This strategy requires ensuring that access rights remain limited to only those necessary to perform an individual's current job function. The process control, cyber security, and IT industries support the principle of least privilege by using role-based assignment of user privileges. Clarify whether the [SITE/LICENSEE] uses role-based assignment of user privileges, or describe the process used to minimize the adverse impact to site's SSEP functions through management of user account privileges.	Section 1.2, "Account Management," regards authentication, not authorization. Section 1.6, "Least Privilege" addresses authorization and ensures least privilege. A change to NEI 08-09 has been identified to address the question of frequency. Baseline configuration disables unnecessary accounts. Comparing physical and electronic access is an inappropriate comparison. Configuration management and design mod processes support risk mitigation of this threat. Quarterly is appropriate. Quarterly is consistent with high assurance of adequate protection.	Revise NEI 08-09, Revision 3, Appendix D, Section 1.2, "Account Management," Add the following bullets: • requiring access rights to be job function based, • conducting reviews when as individuals job function changes to ensure that rights remain limited to the individuals job function, reviewing and documenting CDA accounts at least every 92 days
40. 10 CFR 73.54(c)(1) requires the licensee to implement security controls to protect the digital assets within the scope of the rule from cyber attacks. 10 CFR 73.54(c)(2) requires the licensee to apply and maintain defense-in-depth protective strategies to ensure the	A change to NEI 08-09 has been identified to address the question of frequency.	Revise NEI 08-09, Revision 3, Appendix D, Section 1.4 as follows: 1.4 INFORMATION FLOW ENFORCEMENT This Technical cyber security control: • Enforces and documents assigned

capability to detect, respond to, and recover from cyber attacks. 10 CFR 73.54(c)(3) requires the licensee to mitigate the adverse affects of cyber attacks. 10 CFR 73.54(e)(2) requires the licensee's Cyber Security Plan (CSP) to include description of how the licensee will: (i) Maintain the capability for timely detection and response to cyber attacks; (ii) Mitigate the consequences of cyber attacks; (iii) Correct exploited vulnerabilities; and (iv) Restore affected systems, networks, and/or equipment affected by cyber attacks. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. Additionally, 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(4) require that the licensees' cyber security programs be designed to implement security controls to protect critical digital assets. Appendix D, Section 1.4, "Information Flow Enforcement," of the [SITE/LICENSEE] Cyber Security Plan states that it "Maintains documentation that demonstrates the analysis and addressing of permissible and impermissible flow of information between critical digital assets, security boundary devices		authorizations for controlling the flow of information, in near-real time, within CDAs and between interconnected systems in accordance with the established defensive strategy. • Maintains documentation that demonstrates the analysis and addressing of permissible and impermissible flow of information between CDAs, security boundary devices and boundaries and the required level of authorization to allow information flow as defined in the defensive strategy. • Implements and documents information flow control enforcement using protected processing level as a basis for flow control decisions. • Implements near-real time capabilities to detect, deter, prevent, and respond to illegal or unauthorized information flows. • Prevents encrypted data from bypassing content-checking mechanisms. • Implements one-way data flows using hardware mechanisms, implementing dynamic information flow control based on policy that allows or disallows information flows based on changing conditions or operational considerations. • Implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow

and boundaries and the required level of authorization to allow information flow as defined in the defensive strategy," and that it "Implements and documents information flow control enforcement using protected processing level as a basis for flow control decisions." Effective information flow enforcement should be supported by at least the following: • near-real time capabilities that detect, deter, prevent, and respond to unauthorized information flows as they occur; • use of hardware mechanisms to enforce one-way data flow between defensive levels where critical digital assets are located; and • implementation of controls to prevent traffic encryption from being used to block message content checking Clarify and/or describe the process used by the [SITE/LICENSEE] to support information flow enforcement to detect, deter, prevent, and respond to unauthorized information flows in near-real time, enforce one-way data flow between defensive levels where critical digital assets are located, and prevent traffic encryption from being used to block message content checking.		control decisions. • Configures CDAs such that user credentials are not transmitted in clear text, and documents this requirement in the access control policy.
41 – N/A – No RAI	N/A	N/A

42. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(4) require that the licensees' cyber security programs be designed to implement security controls to protect digital assets from cyber attacks. Appendix D, Section 1.17, "Wireless Access Restrictions," of the [SITE/LICENSEE] Cyber Security Plan states that the cyber security program "establishes usage restrictions and implementation guidance for wireless technologies," and "documents, justifies, authorizes, monitors, and controls wireless access to critical digital assets and ensures that the wireless access restrictions are consistent with defensive strategies developed through the risk assessment process" Wireless communications technology is always subject to external interference and interception. Additionally, it is difficult to define the boundary of a device that use wireless communication technology and identify those devices that have a pathway to the device. Describe how and why usage restrictions and implementation guidance for wireless technologies ensure that security effectiveness is not adversely impacted. The explanation should include why and how the usage	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix D, Section 1.17, "Wireless Access Restrictions" as follows: Add the following bullet: • Prohibits the use of wireless technologies for CDAs associated with safety-related and important-to-safety functions.

restrictions and implementation guidance for wireless technologies provide the same level of isolation between defensive levels as hard-wired technologies. Note that any wireless device that provides a pathway to critical a digital asset (CDA) should itself be considered a CDA. In addition to other devices, equipment or systems connected to such wireless devices could be considered as CDAs. Clarify how protective measures are applied consistently within the same security level. The explanation should describe how the licensee determines what protective measures are applied to a CDA and why the measures are applied.		
43. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and (4) require that the licensees' cyber security programs be designed to implement security controls to protect the assets identified by paragraph (b)(1) from cyber attacks. Appendix D, Section 1.17, of [SITE/LICENSEE] Cyber Security Plan (CSP), "Wireless Access Restrictions," does not address disabling the integral wireless capabilities of critical digital assets (CDAs) that will not be using those capabilities. When the wireless capabilities of CDAs are not disabled, they provide a pathway for cyber attack. If the [SITE/LICENSEE]	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix D, "Wireless Access Restrictions" as follows: Add the following bullet. • disabling wireless capabilities when not utilized,

disables the integral wireless capabilities of CDAs as part of their cyber security program, describe this in the CSP. If not, describe why leaving integral wireless capabilities enabled in CDAs would not provide pathways that an adversary could use to gain access.		
44. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and (4) require that the licensees' cyber security programs be designed to implement security controls to protect the assets identified by paragraph (b)(1) from cyber attacks. Appendix D, Section 1.17, "Wireless Access Restrictions," of the [SITE/LICENSEE] Cyber Security Plan, discusses conducting "scans for unauthorized wireless access and disabling access points if unauthorized access points are discovered." Describe the process by which the [SITE/LICENSEE] will determine the frequency of scans for unauthorized wireless devices.	A change to NEI 08-09 has been identified to address this concern. Licensee design and configuration management programs provide extensive oversight in this area. Plant changes are too rigorous to warrant a more frequent review. Physical access and IMP controls further mitigate this vector. Annually is consistent with high assurance of adequate protection.	Revise NEI 08-09, Revision 3, Appendix D, Section 1.17 as follows: Revise the final bullet to read: Conducts scans every 12 months for unauthorized wireless access points in accordance with this document and disables access points if unauthorized access points are discovered.
45. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(4) require that the licensees' cyber security program be designed to Implement	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix D, Section 1.19 as follows: Revise the final bullet to read: • Enforces and documents mobile devices are used in one security level and mobile devices are not moved between security levels ~~unless governed by the M&TE~~

security controls to protect digital assets from cyber attacks. Appendix D, Section 1.19, of the [SITE/LICENSEE] Cyber Security Plan (CSP) describes "access control for portable and mobile devices." The last bullet states that the cyber security program: "Enforces and documents mobile devices are used in one security level and mobile devices are not moved between security levels unless governed by the M&TE [Measuring & Test Equipment] program or equivalent." Describe how and why the M&TE program ensures that security effectiveness is not adversely impacted by moving mobile devices between security levels. The explanation should include why and how the M&TE program provides the same level of isolation between security levels as the absence of the portable and mobile devices that move between security levels. Note that portable and mobile devices would provide pathways to critical digital assets (CDAs) if they are connected to them. Therefore, those portable and mobile devices should themselves be CDAs. In addition, other devices, equipment or systems connected to portable and mobile devices could be CDAs. Are protective measures applied consistently within the same defensive level? If so clarify this in the [SITE/LICENSEE] CSP. If not, describe how protective measures are applied to these CDAs. How has the MT&E program been augmented		~~program or equivalent~~.

to provide high assurance that the mobile devices are secure?		
46. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix D, Section 1.22, of the [SITE/LICENSEE] Cyber Security Plan (CSP) describes the "Use of External Systems." It also states that the cyber security program: "Establishes the terms and conditions to securely manage and restrict external system access from higher levels" and "establishes the terms and conditions to securely manage and restrict external system access to critical digital assets in the higher levels." For the defensive architecture to protect critical digital assets (CDAs) effectively from cyber attacks, protective measures must be applied consistently within the same defensive level. Two-way communication between higher and lower defensive levels defeats the purposes of establishing defensive levels to isolate a network that includes CDAs from other networks. Describe why and how the terms and conditions to securely manage and restrict external system access from higher levels	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix D, Section 1.22 as follows: Replace the first two bullets with the following: • Ensures that external systems cannot be accessed from higher levels, such as Levels 4 and 3, • Prohibits external systems from accessing CDAs in Levels 3 and 4, and

would provide the same level of isolation between the higher level and other levels as prohibiting communications between the external systems and the CDAs located in the higher levels. Describe why and how the terms and conditions to securely manage and restrict external system access to CDAs in the higher levels would provide the same level of isolation between the higher level and other levels as prohibiting communications between the external systems and the CDAs located in the higher levels. If the external systems are connected to a CDA or a network to which a CDA is connected, the external systems should themselves be considered CDAs. Additionally, any assets connected to the external systems may be CDAs. Are protective measures applied consistently within the same security level? If so clarify this in the [SITE/LICENSEE] Cyber Security Plan. If not, describe what protective measures are applied to a CDA and why.		
47. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. The [SITE/LICENSEE] Cyber Security Plan (CSP) does not address how "Publicly Accessible Content Controls" reduce the possibility of sensitive information being made accessible to the public. One of the most commonly used	A change to NEI 08-09 has been identified to address this concern. Release of information to a public domain is done by corporate functions, using policies and procedures that are independent of the nuclear organization. These folks do not have access to sensitive nuclear information. Nuclear would not designate a person to perform this function.	Revise NEI 08-09, Revision 3, Appendix D to add the following control: 1.23 Public Access Protections This security control ensures that information that could cause an adverse impact on SSEP functions or could assist an adversary in carrying out an attack is not released to the public.

strategies to aid in devising a cyber attack is to seek out sources of publicly accessible information. Effective management of publicly accessible information or content is essential to prevent sensitive information from being unintentionally (or intentionally) disclosed. It is essential to monitor, manage, and restrict the sensitive information that is provided to the public. Describe in the CSP how the [SITE/LICENSEE] will manage and implement Publicly Accessible Content Controls to reduce the possibility of sensitive information being made accessible to the public.	Existing laws, regulations, orders, and guidance documents preclude the release of sensitive information to the public, including: • SECY 04-0191, RIS 2005-26, and RIS 2006-31 provide guidance for withholding SUNSI • SECY 05-0091 Provides guidance on public disclosure of SRI. • 10 CFR 2.390 governs public disclosure of non-safeguards sensitive information • 10 CFR73.21 governs disclosure of Safeguards information	
48. 10 CFR 73.54(c)(1) requires the licensee to implement security controls to protect the digital assets within the scope of the rule from cyber attacks. 10 CFR 73.54(c)(2) requires the licensee to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks. 10 CFR 73.54(c)(3) requires the licensee to mitigate the adverse affects of cyber attacks. 10 CFR 73.54(e)(2) requires the licensee's Cyber Security Plan (CSP) to include a description of how the licensee will: (i) Maintain the capability for timely detection and response to cyber attacks; (ii) Mitigate the consequences of cyber attacks;	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix D, Section 2.2, "Auditable Events," as follows: • Configures CDAs so that auditable events are adequate to support after-the-fact investigations of security incidents, and

(iii) Correct exploited vulnerabilities; and (iv) Restore affected systems, networks, and/or equipment affected by cyber attacks. Appendix D, Section 2.2, "Auditable Events," of the CSP states that the auditable events control "Configures critical digital assets so that auditable events to support after-the-fact investigations of security incidents." This sentence appears to missing some words. Please clarify how configuring critical digital assets (CDAs) so that auditable events are preserved and adequate to support after-the-fact investigations of security incidents, Also please clarify how the [SITE/LICENSEE]'s cyber security program will ensure the collection, storage, and preservation of auditable events for CDAs.		
49. 10 CFR 73.54(c)(1) requires the licensee to implement security controls to protect the digital assets within the scope of the rule from cyber attacks. 10 CFR 73.54(c)(2) requires the licensee to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks. 10 CFR 73.54(e)(2) requires the licensee's Cyber Security Plan (CSP) to include a description of how the licensee will: (i) Maintain the capability for timely	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix D, Section 2.2, "Auditable Events" as follows: Add the following bullet: • Includes execution of privileged functions in the list of events to be audited by the CDAs,

detection and response to cyber attacks; (ii) Mitigate the consequences of cyber attacks; (iii) Correct exploited vulnerabilities; and (iv) Restore affected systems, networks, and/or equipment affected by cyber attacks. Recording privileged functions in the list of events to be audited by the critical digital assets is essential for identifying the mechanisms used, and vulnerabilities exploited, in both attempted and successful cyber attacks. However, Appendix D, Section 2.2, "Auditable Events," of the [SITE/LICENSEE]'s CSP does not include the collection of such information. Describe the process by which [SITE/LICENSEE]'s cyber security program will enable an audit trail for programmatic execution of privileged functions and how associated audit records will be correlated with the user who initiated the program or script.		
50. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(4) require that the licensee's cyber security program be designed to implement security controls to protect the digital assets identified by paragraph 10 CFR 75.54(b)(1) from cyber attacks. 10 CFR 73.54(e)(2)	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix D, Section 2.8, "Time Stamps," as follows: Replace the entire section to read: 2.8 Time Stamps This Technical cyber security control ensures CDAs use a time source protected at an equal or greater level than the CDAs or internal system clocks to generate time stamps for

requires the licensee's Cyber Security Plan (CSP) to include a description of how the licensee will: (i) Maintain the capability for timely detection and response to cyber attacks; (ii) Mitigate the consequences of cyber attacks; (iii) Correct exploited vulnerabilities; and (iv) Restore affected systems, networks, and/or equipment affected by cyber attacks. Appendix D, Section 2.8, "Time Stamps," of the CSP states "This technical cyber security control ensures that critical digital assets use internal system clocks to generate time stamps for audit records as identified by the critical digital asset risk assessment." Since internal system clocks drift, high assurance of synchronized time stamps can not be achieved by their use. How does [SITE/LICENSEE] ensure that the method(s) selected for such time synchronization do not introduce a vulnerability to cyber attack and common-mode failure? If time synchronization cannot be applied to a CDA, how does [SITE/LICENSEE] implement alternative controls?		audit records, and the time on CDAs are synchronized. The time of CDAs are synchronized from a dedicated source protected at an equal or greater level than the CDA existing on the security network, attached directly to the CDA, or via SNTP and a trusted key management process. Only methods of time synchronization that do not introduce a vulnerability to cyber attack and/or common-mode failure are utilized, or alternative controls are implemented to manage potential cyber security risks when time synchronization cannot be used for a CDA.

51. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks, up to and including the design basis threat. Appendix D, Section 3.1, of the [SITE/LICENSEE] Cyber Security Plan describes "CDA, System and Communications Protection Policy and Procedures" and states that "This Technical cyber security control ensures development, dissemination, and periodic reviews and updates of…" Describe the process by which [SITE/LICENSEE] determines the periodicity of and criteria for this review.	This was responded to in RAI 37.	Please refer to the resolution in the response to RAI 37.
52. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. Additionally, 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(4) require that the licensees' cyber security program be designed to implement security controls to protect digital assets from cyber attacks. Appendix D, Section 3.4, of the [SITE/LICENSEE] Cyber Security Plan (CSP) describes "denial of service (DoS) protection" and states that this technical control "Configures Critical Digital Assets (CDA) to	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix D, Section 3.4 as follows: Revise the final bullet to read: • Configures CDAs to manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding and saturation types of denial-of-service attacks.

protect against or limit the effects of denial of service attacks." This section further states that this technical control "Configures CDAs to manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding-types of denial-of-service attacks." The NRC staff noted that Appendix D, Section 3.4 of the CSP does not address "saturation type" denial of service (DoS) attacks. DoS attacks generally involve consuming or blocking the use of a necessary resource such as network bandwidth, memory, bulk (disk) storage or central processing unit power. It can also involve overwhelming key system components and applications by "saturating" them with large numbers of concurrent, or rapid sequential, service requests (i.e., the typical way that websites are attacked). Clarify how the [SITE/LICENSEE]'s cyber security program protects against, or limits the effects of DoS attacks including "saturation" types of DoS attacks.		
53. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix D, Section 3.15, "Secure Name/Address Resolution Service (Recursive or Caching)" of the [SITE/LICENSEE] Cyber Security Plan states	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix D, Section 3.15, "Secure Name/Address Resolution Service (Recursive or Caching)" as follows. Revise the first bullet as follows: • Configures the systems that serve name/address resolution service for CDAs to perform data origin authentication and data integrity verification on the resolution response

that the security control: "Configures the systems that serve name/address resolution service for critical digital assets to perform data origin authentication and data integrity verification on the resolution response they receive from authoritative sources when requested by critical digital assets as identified by the risk assessment." Implementation of the control ensures that name/address resolution messages that are received must be authenticated and verified irrespective of whether they are specifically requested or not. If requested and unrequested messages are not both authenticated and verified, an adversary can exploit name/address mapping so that message traffic will go to unauthorized destinations. This type of attack is called "DNS [domain name system] cache poisoning." Clarify how the [SITE/LICENSEE]'s cyber security program will include authentication and verification of both types of messages, or describe the process by which [SITE/LICENSEE] will protect against DNS cache poisoning.		they receive from authoritative sources ~~when requested by CDAs as identified by the risk assessment~~.
54. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix D, Section 3.21,	This control was removed from RG 5.71 when published. We will follow suit and delete the control to maintain alignment.	Revise NEI 08-09, Revision 3, Appendix D, to delete Section 3.21, "Abstraction Techniques."

"Abstraction Techniques," of [SITE/LICENSEE]'s Cyber Security Plan describes the use of abstraction techniques to deploy a diverse set of operating systems and applications. Describe the process by which [SITE/LICENSEE] employs abstraction techniques (e.g., virtualization) to create effective diversity, particularly if the underlying critical digital asset hardware platform and base hypervisor software are actually homogeneous?		
55. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks. A basic cyber security control is to design systems to fail in a known and desirable state to minimize the adverse impact the system failure has on other functions (i.e., preventing a loss of confidentiality, integrity, or availability). This design principle is particularly important for critical digital assets (CDAs) which by definition are associated with site safety, security, and emergency preparedness (SSEP) functions. The [SITE/LICENSEE] Cyber Security Plan does not address this control. Describe how the licensee's cyber security program addresses CDA failures and compromises to (1) minimize the adverse impact to the site's SSEP functions and (2) prevent a loss of CDA confidentiality, integrity, or availability.	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix D, Section 3 as follows: Add the following new control to Section 3 of Appendix D: Fail in Known (Safe) State This cyber security control ensures the following: • CDAs fail in a state that ensures that SSEP functions are not adversely impacted by the CDA's failure, and • A loss of availability, integrity, or confidentiality, in the event of a failure of the CDA or a component of the CDA is prevented.

56. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix D, Section 4.1, "Identification and Authentication Policies and Procedures "of the [SITE/LICENSEE] Cyber Security Plan (CSP) states that the authentication policy and procedures will "uniquely identify users," and will permit "verifying the identity of users." The CSP does not address the ability to uniquely identify processes acting on behalf of a user, in addition to the user himself/herself. Clarify that Appendix D, Section 4.1, of the CSP provides controls for auditing and identifying processes running on behalf of a user, or describe how the cyber security program addresses and provides for the user identification and activity auditing of processes running on behalf of a user.	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix D, Section 4.1, "Identification and Authentication Policies and Procedures" as follows: Revise the first two bullets of the second bulleted list in the section to read: • Uniquely identifying users, and processes acting on behalf of a user, • Verifying the identity of users, and processes acting on behalf of a user,
57. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix D, Section 4.6, "Identifier Management," of the [SITE/LICENSEE] Cyber Security Plan states that user identifiers will be disabled after a	A change to NEI 08-09 has been identified to address this concern. Inactivity is a poor measure, as many systems are very infrequently used. When no longer needed is more appropriate, and can be tied to management controls.	Change NEI 08-09, Revision 3, Appendix D, "Identifier Management", Section 4.6 as follows: • ~~Disabling the user identifier after 30 days of inactivity; and~~ • Disabling user identifier within 31 days after the identifier is not longer needed; and

"defined time period of inactivity." Explain the process by which the maximum defined period of inactivity is determined, and, if appropriate, the actual time period established.		
58. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(4) require that the licensee's cyber security program be designed to implement security controls to protect digital assets. Appendix D, Section 5.1, "Removal of Unnecessary Services and Programs," of the [SITE/LICENSEE] Cyber Security Plan (CSP) addresses a range of "hardening" steps that will be applied to critical digital assets (CDAs). The NRC staff notes that the CSP does not address the elimination or disabling of device drivers for unused peripherals and unused removable media support. Clarify if the removal of unnecessary services and programs includes the elimination or disabling of device drivers for unused peripherals and unused removable media support. If not, describe how device drivers for unused peripherals and unused removable media support are addressed in the CSP to prevent an adversary from exploiting them.	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix D, Section 5.1, "Removal of Unnecessary Services and Programs" as follows: Add the following two bullets to the existing list in the section: • Device drivers for unused peripherals • Unused removable media support
59. 10 CFR 73.54(a)(1) requires the licensee	A change to NEI 08-09 has been	Revise NEI 08-09, Revision 3, Appendix D,

to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks. 10 CFR 73.54(c)(2) require that the licensees' cyber security program must be designed apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks. Finally, 10 CFR 73.54(e)(2) requires that the cyber security plan (CSP) must include measures for incident response and recovery from cyber attacks. Appendix D, Section 5.2, of the [SITE/LICENSEE] CSP states: "Configure host intrusion detection system [HIDS] to include attributes such as: static file names, dynamic file name patterns, system and user accounts, execution of unauthorized code, host utilization, and process permissions to configure the HIDS to meet the security requirements as identified by the risk determination." Please state whether HIDS are configured to detect cyber attacks up to and including the DBT.	identified to address this concern.	Section 5.2 as follows: Revise the first bullet to read as follows: Configure HIDS to include attributes such as: static file names, dynamic file name patterns, system and user accounts, execution of unauthorized code, host utilization, and process permissions to enable the system to detect cyber attacks up to and including the DBT.
60. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(4) require that the	A change to NEI 08-09 has been identified to address this concern.	Change NEI 08-09, Revision 3, Appendix E, Section 1.6, "Media Sanitation and Disposal," as follows: NEI 08-09 Media sanitization and disposal actions are

licensee's cyber security program must be designed to implement security controls to protect the digital from cyber attacks and to ensure that the functions of protected digital assets are not adversely impacted due to cyber attacks. Appendix E, Section 1.6, "Media Sanitation and Disposal," of the [SITE/LICENSEE] cyber security plan discusses that methods are periodically tested to verify proper functioning. Please describe how the period for testing is determined.		tracked, documented, and verified, and every 92 days tests are performed on sanitized data to ensure equipment and procedures are functioning properly.
61. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(4) require that the licensee's cyber security program be designed to implement security controls to protect the digital assets from cyber attacks and to ensure that the functions of protected digital assets are not adversely impacted due to cyber attacks. Appendix E, Section 3.2, "Flaw Remediation" of the [SITE/LICENSEE] cyber security plan (CSP) discuses "flaw remediation." The [SITE/LICENSEE]'s CSP indicates that software updates to correct flaws following the configuration management process. The [SITE/LICENSEE] CSP is not clear whether the configuration management process will include testing to verify that the updates actually correct the targeted flaw/vulnerability. Please	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix E, Section 3.2, "Flaw Remediation" as follows: Replace the entire section with the following: This security control establishes, implements, and documents procedures to: • 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. Before implementing corrections, software updates related to flaw remediation are documented and tested to determine the effectiveness and potential side effects on CDAs. Flaw remediation information is

describe how the [SITE/LICENSEE]'s CSP will include testing of a critical digital asset to verify that a flaw has been eliminated before the critical digital asset is returned to operation.		captured in the Corrective Action Program.
62a. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(4) require that the licensee's cyber security program be designed to implement security controls to protect the critical digital assets (CDA) from cyber attacks and to ensure that the functions of digital assets are not adversely impacted due to cyber attacks. Section E.3.3, "Malicious Code Protection," of the [SITE/LICENSEE] Cyber Security Plan (CSP) states: "Malicious code protection software products from multiple vendors are documented and employed as part of defense-in-depth, and the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information systems are addressed." If the information systems include critical digital assets, please clarify this.	RAI 62 had two parts. This will be 62a. A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix E, Section 3.3, "Malicious Code Protection" as follows: Revise the first bullet to read: • Data communication between systems, CDAs, removable media, or other common means; and
62b. - Appendix E, Section 3.4, "Monitoring	RAI 62 had two parts. This will be	Revise NEI 08-09, Revision 3, Appendix E,

Tools and Techniques" of the [SITE/LICENSEE] Cyber Security Plan (CSP) discusses monitoring CDA incidents. To ensure that intrusion detection and prevention tools operate properly, they need to be tested periodically. Please confirm [SITE/LICENSEE] tests intrusion detection and prevention systems to ensure they operate properly. Also specify the frequency of the tests and the basis for the frequency.	62b. A change to NEI 08-09 has been identified to address this concern.	Section 3.4, "Monitoring Tools and Techniques" Add the following as the fourth from the last bullet: Cyber intrusion detection and prevention systems are functionally tested (e.g., test that verifies that signatures are functioning, such as the use of a benign virus signature file) every 7 days, and before being placed back in service after each repair or inoperative state.
63. 10 CFR 73.54 (a) requires the licensee provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix E, Section 3.7, "Software and Information Integrity" of the [SITE/LICENSEE] Cyber Security Plan (CSP) states: "Reassessing and documenting the integrity, operation and functions of software and information by performing regular integrity, operation and functional scans" Although the CSP states that the scans will be regular, it does not describe what this period is, does not include any method of determining this period, and unlike other sections of the CSP where a period or interval is determined using a "risk assessment" process, there is no such commitment. Please provide the frequency at which regular integrity, operational, and functional scans will occur.	A change to NEI 08-09 has been identified to address this concern. Licensee design and configuration management programs provide extensive oversight in this area. Plant changes are too rigorous to warrant a more frequent review. Physical access and IMP controls further mitigate this vector. Every 2 years is consistent with ensuring high assurance of adequate protection.	Revise NEI 08-09, Revision 3, Appendix E, Section 3.7, "Software and Information Integrity" as follows: • Reassessing and documenting the integrity, operation and functions of software and information by performing regular integrity, operation and functional scans, every 24 months, or consistent with manufacturer or vendor recommendations, or as determined by site- specific procedures,

Additionally, describe why the defined period for performing these scans will provide high assurance that the integrity of the critical digital assets has been maintained.		
64. 10 CFR 73.54(a) requires the licensee provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix E, Section 3.8, "Information Input Restrictions" of the [SITE/LICENSEE] Cyber Security Plan (CSP) states: "Checking information for accuracy, completeness, validity, and authenticity as close to the point of origin as possible. Rules for checking the valid syntax of critical digital asset inputs (e.g., character set, length, numerical range, acceptable values) are documented and in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are pre-screened to prevent the content from being interpreted as commands. The extent to which the critical digital asset is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements." Although the licensee has committed to perform this checking, the CSP states that it will only be done to the "*extent to which the*	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix E, Section 3.8, "Information Input Restrictions" as follows: Strike the following text from the section: The extent to which the CDA is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.

CDA is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements." However, the CSP does not describe what the policy is, nor what the operational requirements are, how they will be determined or how they will relate to the security requirements of this plan, this control, and the rule. Describe what organizational policies and operational requirements will be considered in this process and how they will result in a suitably secure level of input checking to ensure critical digital asset cyber security.		
65. 10 CFR 73.54(a) requires the licensee provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix E, Section 8.1, "Contingency Plan," of the [SITE/LICENSEE]'s Cyber Security Plan (CSP) states: "This security control consists of: • Implementing a cyber security contingency plan to maintain the safety, security and emergency preparedness functions by developing and disseminating roles, responsibilities, assigned individuals with contact information, and activities associated with restoring	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix E, Section 8.1, "Contingency Plan," as follows: Add the following bullet to the bottom of the list: • Deploying CDAs such that, in the event of a loss of processing within a CDA or a loss of communication with operational facilities, CDAs will execute predetermined actions (e.g., alert the operator and do nothing, alert the operator and then safely shut down the process, alert the operator and maintain last operational setting).

CDAs after a disruption or failure. • Coordinating contingency plan development with organizations responsible for related plans (e.g., Emergency Plan, Physical Security Plan) and requirements (e.g., Technical Specifications)." Please describe how the CSP addresses deploying critical digital assets (CDA) such that, in the event of a loss of processing within a CDA or a loss of communication with operational facilities, CDA will execute predetermined actions.		
66. 10 CFR 73.54(c)(1) requires the licensee to implement security controls to protect critical digital assets from cyber attacks. Appendix E, Section 9.2, "Awareness Training," of the [SITE/LICENSEE] Cyber Security Plan states: "Loss off signal from control devices" The word "off" in this phrase appears to be a typographical error. If this is a typographical error, correct it. If this is not an error, clarify the meaning of this paragraph.	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix E, Section 9.2, "Awareness Training" as follows: Correct: Loss off signal from control devices To: Loss of signal from control devices
67. 10 CFR 73.54(d)(1) requires the licensee to ensure that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix E, Section 9.3, "Technical Training," as follows: This security control further consists of

necessary to perform their assigned duties and responsibilities. Appendix E, Section 9.3, "Technical Training," of the [SITE/LICENSEE] Cyber Security Plan (CSP) states: "This security control further consists of establishing, implementing and documenting requirements to: • Provide cyber security-related technical training to individuals: • Before authorizing access to CDAs or performing assigned duties, and • When required by policy or procedure changes and plant modifications, and • At a licensee-defined interval, to mitigate risk and to ensure personnel maintain competency." Although the CSP contains a commitment to provide technical training, it does not specify the interval for this training. If the [SITE/LICENSEE]'s training interval is greater than annual, describe this in the CSP. If not, describe the method used to determine the training interval and how it provides high assurance that technical skills and competencies for personnel performing, verifying, and managing activities within the scope of the cyber security program are maintained.		establishing, implementing and documenting requirements to: • Provide cyber security-related technical training to individuals: o Before authorizing access to CDAs or performing assigned duties, and o When required by policy or procedure changes and plant modifications, and o Every 12 months, to mitigate risk and to ensure personnel maintain competency.
68. 10 CFR 73.54(e)(1) requires that the licensee to describe how the requirements of the	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix E, Section 10.3, "Baseline Configuration" as

rule will be implemented and must account for the site-specific conditions that affect implementation. Appendix E, Section 10.3, of the [SITE/LICENSEE] Cyber Security Plan (CSP) describes "Baseline Configuration." A baseline configuration establishes a full detailed accounting of the settings configuration and components of a device. A comprehensive baseline configuration documentation set should include the following: • a current list of all 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 • switch settings of machine components Documentation management for baseline configurations includes: • a log of configuration changes made, • the name of the person who implemented the change, • the date of the change, • the purpose of the change, • any observations made during the course of the change.		follows: Add the following after the first paragraph of the section: 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 Documentation management for baseline configurations includes: • A log of configuration changes made, • The name of the person who implemented the change, • The date of the change, • The purpose of the change, and • Observations made during the course of the change.

Such information is a necessary part of a cyber security program. Additionally, because some support systems and security systems within the scope of the 10 CFR 73.54 may not be covered by the [SITE/LICENSEE]'s current configuration management program, the CSP needs to include the items above. Please clarify that critical digital assets within the scope of the CSP are captured, documented and maintained within the configuration management program,		
69. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix E, Section 11.2, "Supply Chain Protection," of the [SITE/LICENSEE] Cyber Security Plan (CSP) states: "This security control protects against supply chain threats by employing an organization-defined list of measures to protect against supply chain threats to maintain the integrity of the critical digital assets that are purchased. Although the CSP states that the licensee protects against supply chain threats, it does not clarify what measures the [SITE/LICENSEE] will use to protect against these threats. Please describe how the [SITE/LICENSEE] will protect the integrity of the supply chain.	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix E, Section 11.2, "Supply Chain Protection," as follows: Revise Section 11.2 to read as follows: This security control protects against supply chain threats by employing following measures to protect against supply chain threats and to maintain the integrity of the CDAs that are acquired: • Establishment of trusted distribution paths, • Validation of vendors, and • Requirement of tamper proof products or tamper evident seals on acquired products. Delete the following: "A risk assessment of product acquisitions is performed and heterogeneity is used to mitigate the threat associated with

		vulnerabilities in a single vendor's product, etc."
70. 10 CFR 73.54 (a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix E, Section 12, "Evaluate and Manage Cyber Risk" of the [SITE/LICENSEE] Cyber Security Plan (CSP) states: "Scan for vulnerabilities in the [critical digital assets] CDAs at a maximum regular interval and randomly as defined by the risk determination and as necessary when new vulnerabilities affecting the CDAs are identified and reported" Regular vulnerability scans are critical to preventing cyber attacks. Although the CSP states that the vulnerability scans will occur at regular intervals and randomly as defined by the risk determination, the CSP does not define this risk determination process or how the results will be used. Describe how the risk assessment process will lead to establishing time periods for scanning for vulnerabilities that will provide high assurance that the CDAs remain protected from new cyber security threats. If the [SITE/LICENSEE]'s CSP includes the ability to compare the results of vulnerability scans conducted over time, clarify this in the cyber	A change to NEI 08-09 has been identified to address this concern. Given the defense-in-depth nature of the plant including the use of data diodes, the extensive configuration management program, and significant probability that an outage will be needed, regular scans more frequently than 2y on top of scans done randomly and when vulnerabilities are discovered provides little value. Every 24 months for routine scanning is consistent with high assurance of adequate protection. Some CDAs (e.g. cyber security devices) will have shorter intervals, but a vast majority may require outage.	Revise NEI 08-09, Revision 3, Appendix E, Section 12, "Evaluate and Manage Cyber Risk", as follows: Change the first bullet to read: • Scan for vulnerabilities in the CDAs no less frequently than every 24 months, and at random intervals, and as necessary when new vulnerabilities affecting the CDAs are identified and reported;

security plan. If not, describe how the licensee's CSP will manage the security controls, flaw remediation activities, and vulnerability management processes to protect critical digital assets from new vulnerabilities and the ever changing capabilities of cyber attackers. If the [SITE/LICENSEE]'s CSP includes a vulnerability scanning process that supports a comprehensive range of attack modalities and CDA platforms, clarify this in the cyber security plan. If not, describe how the employed vulnerability scans will provide high assurance that CDAs are protected up to the DBT. Also please explain how vulnerability scans are conducted and how the cyber security program uses the results of vulnerability scans.		
71. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are protected against cyber attacks. Appendix E, Section 3.5 "Security Alerts and Advisories" of the [SITE/LICENSEE] Cyber Security Plan states: "…Based on plant and business operational requirements, independently evaluating and determining the need, severity, methods and time frames for implementing security directives consistent with the cyber security controls for the critical digital asset…" However, the plant and business operational requirements may not be consistent with the	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix E, Section 3.5 "Security Alerts and Advisories" as follows: Revise the second bullet as follows: ~~Based on plant and business operational requirements, I~~ Independently evaluating and determining the need, severity, methods and time frames for implementing security directives consistent with the cyber security controls for the CDA.

security requirements. Please explain how cyber security considerations are factored into the determination of the need, severity, methods and time frames for implementing security directives.		
72. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks. 10 CFR 73.54(c)(1) and (4) require that the licensee's cyber security program be designed to implement security controls to protect digital assets from cyber attacks and to ensure that the functions of protected assets are not adversely impacted due to cyber attacks. Additionally, 10 CFR 73.54(c)(2) requires licenses to ensure the capability to respond to cyber attacks, and 10 CFR 73.54(e)(2) states that the plan must include measures for incident response and recovery from cyber attack. A critical element of an incident response is the development, implementation, and maintenance of an incident response plan and all its associated components. Although the [SITE/LICENSEE]'s Cyber Security Plan (CSP) describes some aspects of incident response and attack mitigation, and also includes a specific commitment to develop a contingency plan, the CSP does not commit the [SITE/LICENSEE] to develop a cyber incident and attack response plan. Please describe whether the licensee will develop a cyber incident and attack response plan to comply with the requirements of the rule. If not, why not?	Title 10 of the Code of Federal Regulations, Part 73, Section 73.54(e)(2) states: The cyber security plan must include measures for incident response and recovery for cyber attacks. Accordingly, NEI 08-09, Revision 3, Appendix A, "Cyber Security Plan Template," Section 4.6, "Attack Mitigation and Incident Response" describes the measures licensees use for attack mitigation and incident response.	No change necessary.

73. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and (4) require that the licensee's cyber security program be designed to implement security controls to protect digital assets cyber attacks and to ensure that the functions of protected assets are not adversely impacted due to cyber attacks. The [SITE/LICENSEE] Cyber Security Plan (CSP), Appendix E, Section 10.6, "Access Restrictions for Change," states: "Employs automated mechanisms to enforce access restrictions and to support subsequent audits of enforcement actions." The intent of automated mechanisms is to (1) detect and prevent unauthorized changes, (2) enforce access restrictions, and (3) to support subsequent audits of enforcement actions. However, the CSP does not appear to contain a commitment to detect and prevent unauthorized changes. For example, cyber attacks might result in a change to the configuration of a critical digital asset without the change going through the configuration management or authentication processes (a virus for example); using automated mechanisms. If the use of the "automated mechanisms" in the sentence above includes using automated mechanisms to detect unauthorized changes to critical digital assets, clarify this in the CSP. If	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix E, Section 10.6, "Access Restrictions for Change," as follows. Revise the paragraph in question as follows. Employs automated mechanisms to detect unauthorized changes, to enforce access restrictions and to support subsequent audits of enforcement actions

not, describe how such unauthorized changes to critical digital assets would be detected by automated mechanisms.		
74. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. 10 CFR 73.54(c)(1) and (4) require that the licensee's cyber security program be designed to implement security controls to protect the assets identified by paragraph (b)(1) from cyber attacks and to ensure that the functions of protected assets identified by paragraph (b)(1) are not adversely impacted due to cyber attacks. Additionally, 10 CFR 73.54(c)(2) requires the licensee to maintain the capability to recover from cyber attacks. Appendix E, Section 8.2, "Contingency Plan Testing," of the [SITE/LICENSEE] Cyber Security Plan (CSP) appears to omit post attack forensic analysis for determining methods of attacks and determining the extent of compromise of critical digital assets and Safety, Security and Emergency Preparedness (SSEP) functions for the purpose ensuring that the same attack vector will not succeed in the future. What post-attack actions would [SITE/LICENSEE] take to analyze the methods used by the attacker to determine the extent of compromise of critical digital assets and SSEP functions to prevent the same attack vector from succeeding in the future?	The cause analysis performed under the Corrective Action Problem answers the "why" question until an understanding of how to mitigate the issue has been discovered. A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix E, Section 7.4, "Incident Handling" as follows: Revise: Description of individual postulated classes or categories of incidents or attacks as analyzed during ~~assessment methodology, and indicators and potential/planned methods of mitigation~~. To: Description of individual postulated classes or categories of incidents or attacks as analyzed during the Cause Analysis performed under the Corrective Action Program (e.g. common cause, apparent cause, root cause).

75. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. 10 CFR 73.54(c)(1) and (4) require that the licensee's cyber security program be designed to implement security controls to protect the assets identified by paragraph (b)(1) from cyber attacks and to ensure that the functions of protected assets identified by paragraph (b)(1) are not adversely impacted due to cyber attacks. Additionally, 10 CFR 73.54(c)(2) requires the licensee to maintain the capability to recover from cyber attacks. The preamble to Appendixes D and E of the [SITE/LICENSEE] Cyber Security Plan (CSP) states: "When implementing alternate compensating controls for a security control, the compensating control is considered applied when there is high assurance that the [critical digital asset] CDA is adequately protected from risks associated with the control that is not applied." This statement appears to contradict the process described in CSP Appendix A, Section 3.1.6, "Mitigation of Vulnerabilities and Application of	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendices D and E Preamble as follows: Delete the sentence: When implementing alternate compensating controls for a security control, the compensating control is considered applied when there is high assurance that the CDA is adequately protected from risk associated with the control that is not applied. And add a clarifying sentence. The preamble, in its entirety, would then read: The Technical Cyber Security Controls in this appendix represent methods for the mitigation of risks to digital systems. When implementing cyber security controls, discretion may be taken with the means by which the control is implemented. When a control or aspects of a control are not implemented, an analysis is performed to ensure that the risk is effectively mitigated. A security control is considered to be applied when there is high assurance that the CDA is adequately protected from the risk considered by the security control. Section 3.1.6 of the NEI 08-09, Revision 3, Appendix A, provides a multi-step process for the analysis and documentation of the application of cyber security controls.

Cyber Security Controls," which states: "For CDAs, the information in Sections 3.1.3 - 3.1.5 is utilized to analyze and document one or more of the following: 1. Implementing the cyber security controls in Appendices D and E of NEI 08-09, Revision 3. 2. Implementing alternative controls/countermeasures that eliminate threat/attack vector(s) associated with one or more of the cyber security controls enumerated in (1) above by: a. Documenting the basis for employing alternative countermeasures; b. Performing and documenting the analyses of the CDA and alternative countermeasures to confirm that the countermeasures provide the same or greater cyber security protection as the corresponding cyber security control; and c. Implementing alternative countermeasures that provide at least the same degree of cyber security protection as the corresponding cyber security control. Not implementing one or more of the cyber security controls by performing an analyses of the specific cyber security controls for the CDA that will not be implemented to provide a		

documented justification demonstrating the attack vector does not exist (i.e., not applicable) and therefore those specific cyber security controls are not necessary." The process described in CSP Appendix A Section 3.1.6 states that the alternate compensating controls will provide equivalent protection to the control that is not implemented. Please clarify which method the licensee will use (i.e., the process described in the preamble to Appendix D and E, or the process stated in Section 3.1.6). Also, please explain how the licensee will ensure that these alternate/compensating controls provide an equal level of protection as the control that was not applied.		
76. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and (4) require that the licensees' cyber security program be designed to implement security controls to protect the assets identified by paragraph (b)(1) from cyber attacks and to ensure that the functions of protected assets identified by paragraph (b)(1) are not adversely impacted due to cyber attacks. Appendix E, Section 11.3, "Trustworthiness," of the [SITE/LICENSEE] Cyber Security Plan (CSP) states:	A change to NEI 08-09 has been identified to address this concern.	Revise NEI 08-09, Revision 3, Appendix E, Section 11.3, "Trustworthiness" as follows: Revise the section as follows: This security control requires that ~~the information system~~ CDAs meet~~s~~ defined levels of trustworthiness and requires that software developers employ software quality and validation methods to minimize flawed or malformed software.

"This security control requires that the information system meets defined levels of trustworthiness and requires that software developers employ software quality and validation methods to minimize flawed or malformed software." Please clarify if the phrase "information system" is a typographical error and the term "critical digital asset" was intended. If "information system" was intended, please explain what is meant by this term and how it relates to the CSP.		