Responses – Generic RAIs on NEI 08-09, Revision 3, Appendix A

NRC Comment / RAI	Response Considerations and Additional Information	Proposed Changes to NEI 08-09
7. (25.) 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. Section 4.3, "Defense-in-Depth Protective Strategies," of the [Site/Licensee] Cyber Security Plan (CSP) discusses restricting communications from lower defensive levels to higher defensive levels however does not elaborate how these communications will be restricted. Explain how communications from lower defensive levels to higher defensive levels will be restricted.	A change to the Plan has been identified to address this concern.	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

NRC Comment / RAI	Response Considerations and Additional Information	Proposed Changes to NEI 08-09
		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 the greatest degree of security are located within the greatest number or strength of boundaries. The criteria below are utilized in the defensive architecture. [• CDAs associated with safety, important to safety and security functions, as well as support systems and equipment which, if compromised, would adversely impact safety, important to safety and security functions, are allocated within the defensive architecture to adequately protect them and the plant against cyber attack while permitting them to perform their design function. • Data flow from the Level 4 to lower levels and from Level 3 to lower levels is initiated from the higher level, with the following exceptions. o Data flow initiated from Level 3 to Level 4 is permitted if isolation is accomplished by

NRC Comment / RAI	Response Considerations and Additional Information	Proposed Changes to NEI 08-09
		the use of a data diode, or other deterministic equivalent, between Levels 3 and Level 2. (Any data flow to Level 4 from Level 2 or lower is deterministically eliminated by the isolation.) o Data flow may be initiated in either direction between level 3 and lower levels to accommodate other regulatory requirements and provided the level 3 instance is isolated from any other Level 3 or Level 4 instance. • Data only flows from one level to other levels through a device or devices that enforce security policy between each level. • Maintains the capability to detect, prevent, delay, mitigate, and recover from cyber attacks. • CDAs are configured as described in the security controls applicable to that CDA. • Applications, services, and protocols not necessary to support the design-basis function of the contained CDAs are evaluated and eliminated if appropriate.]

NRC Comment / RAI	Response Considerations and Additional Information	Proposed Changes to NEI 08-09
		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."
8. (26.) 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. Section 4.3, "Defense-in-Depth Protective Strategies," of the [Site/Licensee] Cyber Security Plan discusses protective strategies. Explain how the defensive architecture, in addition to the security controls, manages communications between defensive levels and how the defensive architecture maintains the capability to detect, prevent, delay, mitigate, and recover from cyber attacks.	Addressed with Draft Generic RAI 7, above.	No change required to NEI 08-09 beyond those made for Draft Generic RAI 7, above.
35. 10 CFR 73.54(b)(2) requires the licensee to establish, implement, and maintain a cyber security program for the protection of the critical digital assets. Section 2.2, "Performance Requirements" provides a	A change to the Plan has been identified to address this concern.	1. Amend NEI 08-09, Revision 3, Appendix A, Section 4.9 to read: *Cyber risk is evaluated and managed utilizing*

NRC Comment / RAI	Response Considerations and Additional Information	Proposed Changes to NEI 08-09
list of performance based requirements for the CSP. The following clarifications are needed: 10 CFR 73.54(e)(2)(ii) states the cyber security plan must describe how the licensee will mitigate the consequences of cyber attacks. Section 2.2.2 states, "Ensure that the Program maintains the capability to detect, respond to, and recover from cyber attacks up to and including the design basis threat of radiological sabotage as stated in §73.1 at all times. (§ 73.55(b)(2)(i), § 73.54(e)(2)(i), and § 73.54(e)(2)(iv))." Clarify whether performance based requirements will include maintaining the capability to mitigate the consequences of cyber attacks as part of cyber attack response capabilities. 10 CFR 73.54(e)(2)(iii) states the cyber security plan must describe how the licensee will correct exploited vulnerabilities. Section 2.2.2 states, "Ensure that the Program maintains the capability to detect, respond to, and recover from cyber attacks up to and including the design basis threat of radiological sabotage as stated in §73.1 at all times. (§ 73.55(b)(2)(i), § 73.54(e)(2)(i), and § 73.54(e)(2)(iv))." Clarify whether performance based requirements will include maintaining the capability to correct exploited vulnerabilities as part of cyber attack recovery capabilities. 10 CFR 73.54(d)(1) states the licensee shall ensure appropriate facility personnel, including contractors, are aware of cyber security requirements and receive	NEI 08-09, Revision 3, Appendix A, Sections 4.9 and 4.10 have been revised to remove the reference to Section 2.2 Performance Requirements. The Performance Requirements will still be contained in Section 2.2, however not directly referenced in Sections 4.9 and 4.10. Additionally, the first sentence in section 4.10 has been revised to add reference to the Rule. NEI 08-09, Revision 3, Appendix A, Section 2.2 has been revised and additional performance based requirements have been added consistent with the language contained in 10 CFR 73.54.	*site programs and procedures ~~outlined in the Performance Requirements in Section 2.2~~.* The phrase "outlined in the Performance Requirements in Section 2.2" is removed. 2. Amend NEI 08-09, Revision 3, Appendix A, Section 4.10 to revise the first sentence and delete the 2nd paragraph: Policies and implementing procedures are developed to meet *the Rule and* implement~~ed~~ cyber security control~~'s~~ objectives provided in Appendices D and E of NEI 08-09, Revision 3… ~~*Policies and implementing procedures are developed in accordance with the Performance Objectives in Section 2.2.*~~ 3. NEI 08-09, Revision 3, Appendix A, Section 2.2 has been re-written and re-organized to align with 10CFR 73.54 as shown below: 2.2.1 Evaluate modifications to CDAs prior to implementation to achieve high assurance that digital computer and communications systems and networks are adequately protected against cyber attacks, up to and including the DBT. (§ 73.54(a)(1) and

NRC Comment / RAI	Response Considerations and Additional Information	Proposed Changes to NEI 08-09
the training necessary to perform their assigned duties and responsibilities. Clarify whether performance based requirements will include training facility personnel, including contractors, to be aware of cyber security requirements training necessary to perform their assigned duties and responsibilities. 10 CFR 73.54(d)(3) states the licensee shall ensure that modifications to critical digital assets are evaluated before implementation to ensure that the cyber security performance objectives identified in paragraph (a)(1) of the Rule are maintained. Clarify whether performance based requirements will include evaluation of modifications to CDAs prior to implementation to achieve high assurance that digital computer and communications systems and networks are adequately protected against cyber attacks, up to and including the DBT.		§ 73.54(d)(3)). 2.2.2 Prevent adverse impact to SSEP functions resulting from cyber attacks, that would adversely impact the integrity or confidentiality of data and/or software, deny access to systems, services, and/or data, and adversely impact the operation of systems, networks, and associated equipment to protect against the DBT. (§ 73.54(a)(2) and § 73.55(b)(2)) 2.2.3 Analyze digital computer and communications systems and networks and identify those assets that must be protected against cyber attack to preserve the intended function of plant systems, structures, and components within the scope of the Rule and account for these conditions in the design of the Program. (§ 73.54(b)(1) and § 73.55(b)(4)). 2.2.4 Establish, implement and maintain the Program in accordance with §73.54. (§ 73.54(b)(2) and § 73.55(b)(8)). 2.2.5 Incorporate the cyber security program as a component of the physical protection program. (§ 73.54(b)(3) and § 73.55(b)(8)). 2.2.6 Implement security controls to protect the identified assets from cyber

NRC Comment / RAI	Response Considerations and Additional Information	Proposed Changes to NEI 08-09
		attacks (§ 73.54(c)(1)) 2.2.7 Provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure effectiveness of the Program. (§ 73.54(c)(2) and § 73.55(b)(3)(ii)). 2.2.8 Maintain the capability to mitigate the adverse consequences of cyber attacks. (§ 73.54(c)(3) and § 73.54(e)(2)(ii)). 2.2.9 Ensure that the functions of identified protected assets are not adversely impacted due to cyber attacks. (§ 73.54(c)(4)) 2.2.10 Ensure that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training necessary to perform their assigned duties and responsibilities. (§ 73.54(d)(1)). 2.2.11 Use the site corrective action program to: 1) track, trend, correct, and prevent recurrence of cyber security failures and deficiencies, and 2) evaluate and manage cyber risks. (§ 73.54(d)(2) and § 73.55(b)(10)). 2.2.12 Describe how the cyber security program requirements will be

NRC Comment / RAI	Response Considerations and Additional Information	Proposed Changes to NEI 08-09
		implemented; accounting for the site-specific conditions that affect implementation. (§ 73.54(e)(1)) 2.2.13 Ensure that the Program maintains the capability to detect, respond to, and recover from cyber attacks up to and including the design basis threat of radiological sabotage as stated in §73.1 at all times. (§ 73.54(e)(2)(i), § 73.54(e)(2)(iv) and §73.55(b)(2)). 2.2.14 Maintain the capability to correct exploited vulnerabilities. (§73.54(e)(2)(iii)). 2.2.15 Demonstrate the ability to meet Commission requirements through implementation of the Program in licensee policies/procedures which are available upon the request of an authorized representative of the Commission. (§ 73.54(f) and § 73.55(b)(5)). 2.2.16 Review the cyber security program as a component of the physical security program, including the periodicity requirements. (§ 73.54(g) and § 73.55(m)). 2.2.17 Describe how all records and supporting technical documentation are retained. (§ 73.54(h)). 2.2.18 Coordinate implementation of this

NRC Comment / RAI	Response Considerations and Additional Information	Proposed Changes to NEI 08-09
		Plan and associated procedures with other [site/fleet] procedures to preclude conflict during both normal and emergency conditions. (§ 73.55(b)(11)).