Responses – Generic RAIs on NEI 08-09, Revision 3, Appendix A – Supplement 1

Clarifications to several generic RAIs responses submitted to the NRC, by NEI on behalf of the industry, on March 5 and 10, 2010.

NRC Comment / RAI	Response Considerations and Additional Information	Proposed Changes to NEI 08-09
Open Issue One: Defensive Strategy	This response supersedes the response to Draft RAI 7. 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 the greatest degree of security are located within the greatest number or strength of boundaries. The criteria below are utilized in the defensive architecture.

NRC Comment / RAI	Response Considerations and Additional Information	Proposed Changes to NEI 08-09
		[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 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, and 2. • 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 Level 3 and Level 4, 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

NRC Comment / RAI	Response Considerations and Additional Information	Proposed Changes to NEI 08-09
		08-09, Revision 3, Appendix D, Section 1.4. Example 2: - 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, and 3 - 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.”

NRC Comment / RAI	Response Considerations and Additional Information	Proposed Changes to NEI 08-09
Open Issue 2: Time intervals for periodic activities.	All intervals were addressed in the RAIs for the Security Controls. Generic RAI 36 included a modification to Appendix A and the response will be included, below to allow for incorporation of all changes to NEI 08-09, Revision 3, Appendix A with the first round of Generic RAIS. Please see response to RAI 70 for the relevant modification with respect to vulnerability scanning. Revisions to Sections 3.1.2 and 4.7 of NEI 08-09, Revision 3, Appendix A have also been identified.	Revise NEI 08-09, Revision 3, Section 3.1.2 as follows: Performing or overseeing stages of the cyber ~~risk~~ assessment process. Revise NEI 08-09, Revision 3, Section 4.7 as follows: Documented requirements for the replacement of components ~~based on risk determination~~. Please see the response to RAI 36, below, which further elaborates this response.

NRC Comment / RAI	Response Considerations and Additional Information	Proposed Changes to NEI 08-09
Open Issue 3: Storage of records	This response supersedes the response to Draft RAI 28. The section will be revised to clarify the records retention duration for logs.	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, or for as long as practical, within the capability of the CDA. 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

NRC Comment / RAI	Response Considerations and Additional Information	Proposed Changes to NEI 08-09
		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.
Open Issue 4: Critical System definition	The definitions of Critical System (CS) and Critical Digital Asset (CDA) are being revised to maintain alignment with the rule and will be provided in the Glossary. This response supersedes the response to Draft RAI 33. A modification to NEI 08-09, Revision 3,	Revise NEI 08-09, Revision 3, Appendix A, Section 3.1.3, as follows: Replace: • Identifies and documents systems, equipment, communication systems and networks that are associated with the SSEP functions described in § 73.54 (a)(1). Systems, equipment, and network systems associated with these functions are hereafter referred to as critical systems (CS) and are identified in Table 1 of this Plan. CSs are identified by conducting an initial consequence analysis of site systems, equipment, communication systems and networks determine those which, if compromised, exploited or were to fail, could impact the SSEP functions of the nuclear facility without accounting for existing mitigating measures. (Existing mitigating measures are considered when implementing cyber security controls as described in Section 3.1.6.) • Identifies and documents the digital devices or equipment that have a direct or supporting role in the proper functioning of CSs. These digital systems are hereafter called Critical Digital Assets (CDAs). Similar equipment may be

NRC Comment / RAI	Response Considerations and Additional Information	Proposed Changes to NEI 08-09
	Appendix A, Section 3.1.3 will be made accordingly, as specified in this response.	grouped together to form a CDA group, though digital assets within the CDA group are analyzed and protected individually in accordance with Sections 3.1.4 – 3.1.6. With: • Identifies and documents Critical Systems (CS), which must be protected under the Rule. • Identifies and documents Critical Digital Assets (CDAs).
36. 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 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	NEI 08-09 used an expression similar to “as determined by the risk assessment” to indicate two activities: a) that licensees would perform an activity described in a security control if that activity was warranted by a risk assessment. b) that licensees would establish, during the cyber security assessment process, the periodic frequency for performing certain tasks.	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. d) Implementing an alternative frequency or periodicity for the security control employed by documenting the basis for the alternate frequency or periodicity. The basis should include a review of: i) NRC Regulations, Orders

NRC Comment / RAI	Response Considerations and Additional Information	Proposed Changes to NEI 08-09
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,	In the first case, the cyber security controls are implemented in accordance with Section 3.1.6. As such, if the security control is applied, the activity specified in the control will be performed. This allows for simply deleting the, "as determined by the risk assessment" from the security control. Next, in order to address the concern of providing specific frequencies as a baseline in the cyber security controls, two tasks must be accomplished. First, section 3.1.6 of the plan must be	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. Note – Specific modifications to address the list of security controls identified in this RAI will be submitted with the responses to the balance of the generic RAIs on the cyber security controls.

NRC Comment / RAI	Response Considerations and Additional Information	Proposed Changes to NEI 08-09
Appendix E – 1.6 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?	modified to provide licenses a process to tailor that frequency, with justification, during program implementation. Section 4.2 is also modified to maintain consistency with the practices for frequencies in Technical Specifications. The proposed modification to Section 3.1.6 specifies the criteria licensees will use when establishing a time period that is different from that specified in the security control. Second, the security controls in question are to be revised to specify a baseline frequency.	

NRC Comment / RAI	Response Considerations and Additional Information	Proposed Changes to NEI 08-09
	Specific modifications to address the list of security controls identified in this RAI will be submitted with the responses to the balance of the generic RAIs on the cyber security controls.	