

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
<p>1. 10 CFR 73.54 requires the licensee to submit cyber security plans to the NRC. The [Site/Licensee] Cyber Security Plan (CSP) refers to NEI 08-09, Revision 3, Cyber Security Plan for Nuclear Reactors. Various versions of NEI 08-09, Revision 3, were submitted to NRC. What is the date of NEI 08-09, Revision 3, referenced in the CSP? (Note that several licensee CSP submittals incorporate NEI 08-09, Revision 3, and Appendices D & E by reference only).</p>	<p>The cyber security plan template was taken from NEI 08-09, Revision 3 dated September, 2009 as submitted to the NRC for endorsement via letter dated September 15, 2009.</p>	<p>No change required to NEI 08-09.</p>
<p>2. (4.) 10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risks. The [Site/Licensee] Cyber Security Plan (CSP) Section 3.1.2, "Cyber Security Assessment Team,"(CSAT) states that one of the roles and responsibilities of the CSAT is "Evaluating assumptions and conclusions about known cyber security threats; potential vulnerabilities to, and consequences from an attack; the effectiveness of existing cyber security controls, defensive strategies, and attack mitigation methods; cyber security awareness and training of those working with, or responsible for CDAs [critical digital assets] and cyber security controls throughout their system life cycles." Explain how [Site/Licensee] uses the process described above will to stay current on cyber security threats. Please provide a list the sources of cyber security threat information used by [Site/Licensee].</p>	<p>The word, "known" will be removed.</p> <p>Licensee stays current on cyber security threats by implementing Section 4.9.1 of the Plan.</p> <p>A list of sources of threats and vulnerability notices that may be used include those described in Information Notice 2009-24, (e.g. Law enforcement, government agencies, US-CERT, and vendors).</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 3.1.2 as follows:</p> <p>Change: "Evaluating assumptions and conclusions about known cyber security threats"</p> <p>To: "Evaluating assumptions and conclusions about cyber security threats"</p>
<p>3. (14.) 10 CFR 73.54(b)(1) requires the licensee to</p>	<p>The additional details requested</p>	<p>Change NEI 08-09, Revision 3, Section 3.1.3</p>

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
<p>Analyze digital computer and communication systems and networks and identify those assets that must be protected against cyber attacks. Section 3.1.3, "Identification of Critical Assets", of the [Site/Licensee] Cyber Security Plan provides a list of documentation that will be developed for each critical system (CS) examined. Explain how security functional requirements or specifications will be documented with respect to each CS and their associated critical digital assets (CDAs):</p>	<p>will be added to the Plan as indicated.</p>	<p>as follows:</p> <p>For the bulleted list introduced, "For each CS examined, the documentation includes the following," add as the final bullet and sub-bullets:</p> <p>Security functional requirements or specifications, as available, that include the following:</p> <ul style="list-style-type: none"> • information security requirements necessary for vendors and developers to maintain the integrity of acquired systems • secure configuration, installation, and operation of the CDA; • effective use and maintenance of security features/functions; and • known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions, • user-accessible security features/functions and how to effectively use those security features/functions, • methods for user interaction with CDAs, which enables individuals to use the system in a more secure manner, • user responsibilities in maintaining the security of the CDA

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
<p>4. (16.) 10 CFR 73.54(b)(2) requires the licensee to establish, implement, and maintain a cyber security program for the protection of the digital assets. Section 3.1.5, "Tabletop Reviews and Validation Testing," of the [Site/Licensee] Cyber Security Plan states "Performing, where practical, a physical inspection of the connections and configuration of CDAs [critical digital asset], including tracing digital communication connections into and out of the CDA to termination points along digital communication pathways." Explain how physical inspections of connections and configurations of CDAs will trace communication connections into and out of the CDA to each termination point along digital and analog communication pathways.</p>	<p>A change to the Plan has been identified to address this concern.</p>	<p>Revise NEI 08-09, Revision 3, Section 3.1.5, bullet one under "Walkdowns" to read: Performing, where practical, a physical inspection of the connections and configuration of CDAs, including tracing communication connections into and out of the CDA to termination points along communication pathways</p>
<p>5. (20.) 10 CFR 73.54(c)(1) requires the cyber security program to implement security controls to protect the assets identified by paragraph (b)(1) from cyber attacks. Section 3.1.6, "Mitigation of Vulnerabilities and Application of Cyber Security Controls," of the [Site/Licensee] Cyber Security Plan states "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:</p> <ul style="list-style-type: none"> • Performing and documenting the analyses of the 	<p>NRC has indicated that this RAI (Draft RAI Number 5) will be withdrawn.</p>	<p>No change required to NEI 08-09.</p>

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
<p>CDA [critical digital asset] and alternative countermeasures to confirm that the countermeasures provide the same or greater cyber security protection as the corresponding cyber security control."</p> <p>Please describe the process, methods and considerations of the above analyses (e.g., use of "attack vector" analyses,).</p>		
<p>6. (24.) 10 CFR 73.54(c)(1) requires the licensees to implement security controls to protect the assets within the scope of the Rule from cyber attacks. Section 4.2, "Cyber Security Controls," of the [Site/Licensee] Cyber Security Plan (CSP) states "Alternate controls are implemented in situations where a CDA [critical digital asset] cannot support, or the organization determines it is not advisable to implement, a particular cyber security control because that control could adversely impact SSEP [safety, security, and emergency preparedness] functions. Justification for how the selected controls provide an acceptable cyber security capability or level of protection for the CDA is documented. Evaluation and justification is performed and documented." Explain the process and provide the criteria for selecting alternate controls to mitigate the lack of the security control for the CDA in accordance with the process described in Section 3.1.6 and clarify that the justification process is applied to all of the alternate security controls that provide equivalent protection in lieu of the security controls from Appendices D and E</p>	<p>A change to the Plan has been identified to address this concern.</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.2 as follows:</p> <p>Delete the following paragraph from Section 4.2: "Alternate controls are implemented in situations where a CDA cannot support, or the organization determines it is not advisable to implement, a particular cyber security control because that control could adversely impact SSEP functions. Justification for how the selected controls provide an acceptable cyber security capability or level of protection for the CDA is documented. Evaluation and justification is performed and documented."</p>

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
that cannot be implemented.		
<p>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.</p>	<p>A response to this RAI will be submitted to the NRC on or before Wednesday, March 10, 2010.</p>	<p>A response to this RAI will be submitted to the NRC on or before Wednesday, March 10, 2010.</p>
<p>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.</p>	<p>A response to this RAI will be submitted to the NRC on or before Wednesday, March 10, 2010.</p>	<p>A response to this RAI will be submitted to the NRC on or before Wednesday, March 10, 2010.</p>
<p>9. (29.) 10 CFR 73.54(b)(2) requires the licensee to establish, implement, and maintain a cyber security program for the protection of the assets within the scope of the Rule. 10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risks. Section 4.4, "Ongoing Monitoring and Assessment," of the</p>	<p>The cyber security plan in NEI 08-09, Revision 3, Appendix A, Section 4.4, failed to account for rogue assets. Additional information on how rogue assets will be detected is provided in</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.4 as follows: Add the following item to the bulleted list in Section 4.4: "Verification that rogue assets are not</p>

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
<p>[Site/Licensee] Cyber Security Plan (CSP) describes the ongoing monitoring program. Explain how and with what periodicity the [Site/Licensee] will verify that rogue assets have not been connected to the infrastructure.</p>	<p>the cyber security management and operational controls (D-1.18, D-3.6).</p> <p>The verification will happen in accordance with the ongoing monitoring program.</p>	<p>connected to the network infrastructure”</p>
<p>10. (33.) 10 CFR 73.54(d)(3) requires the licensee to ensure that modifications to assets within the scope of the Rule are evaluated before implementation. 10 CFR 73.54(f) requires the licensee to develop and maintain written policies and implementing procedures to implement the cyber security plan. 10 CFR 73.54(g) requires the licensee to review the cyber security program as a component of the physical security program in accordance with the requirements of 10 CFR 73.55(m), including the periodicity requirements. Section 4.4.1, “Configuration Management and Change Control,” of the [Site/Licensee] Cyber Security Plan (CSP) states “A configuration and cyber security life cycle management approach is implemented to update and maintain cyber security controls for CDAs [critical digital assets] in order to ensure that the cyber security program objectives remain satisfied.” Explain the life cycle management approach.</p>	<p>A change to the Plan has been identified to address this concern.</p> <p>The language used in NEI 08-09 was overly broad, as the scope of this rulemaking is plant operations.</p> <p>A change will be made to the Plan to address this error, as specified.</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.4.1 as follows:</p> <p>Delete the words “and cyber security life cycle” from 4.4.1, Paragraph 1, Sentence 2.</p> <p>Add the following as the last paragraph to section 4.4.1: “During the retirement phase, the [Design Control and Configuration Management procedures] address SSEP functions.”</p>
<p>11. (34.) Appendix B to Part 50--Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants, (Criterion) III, “Design Control,” states:</p>	<p>NOTE: There are two items marked 11. This item will be designated 11a.</p> <p>A change to the Plan has been</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.4.1 as follows:</p> <p>Revise Section 4.4.1, Paragraph 2, Sentence 1, to read as follows:</p>

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
<p>Measures shall be established to assure that applicable regulatory requirements and the design basis, as defined in § 50.2 and as specified in the license application, for those structures, systems, and components to which this appendix applies are correctly translated into specifications, drawings, procedures, and instructions. These measures shall include provisions to assure that appropriate quality standards are specified and included in design documents and that deviations from such standards are controlled. Measures shall also be established for the selection and review for suitability of application of materials, parts, equipment, and processes that are essential to the safety-related functions of the structures, systems and components.</p> <p>Measures shall be established for the identification and control of design interfaces and for coordination among participating design organizations. These measures shall include the establishment of procedures among participating design organizations for the review, approval, release, distribution, and revision of documents involving design interfaces.</p> <p>The design control measures shall provide for verifying or checking the adequacy of design, such as by the performance of design reviews, by the use of alternate or simplified calculational methods, or by the performance</p>	<p>identified to address this concern.</p> <p>We are unaware of any Safety Related systems that lack current configuration management documentation or have no configuration management documentation</p> <p>NRC Feedback: Consider referencing Appendix E Control Section 10.</p> <p>Industry Response: NEI 08-09 does reference the Appendix. Section 4.4.1 states: "The configuration management controls described in Appendix E of NEI 08-09, Revision 3, have been implemented as described in Section 3.1.6, and implementation has been documented."</p> <p>Your recommendation has already been accomplished.</p>	<p>"CDA [critical digital asset] cyber security and configuration management documentation is updated or created using site configuration management program or other configuration management procedure or process."</p>

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
<p>of a suitable testing program. The verifying or checking process shall be performed by individuals or groups other than those who performed the original design, but who may be from the same organization. Where a test program is used to verify the adequacy of a specific design feature in lieu of other verifying or checking processes, it shall include suitable qualifications testing of a prototype unit under the most adverse design conditions. Design control measures shall be applied to items such as the following: reactor physics, stress, thermal, hydraulic, and accident analyses; compatibility of materials; accessibility for inservice inspection, maintenance, and repair; and delineation of acceptance criteria for inspections and tests.</p> <p>Design changes, including field changes, shall be subject to design control measures commensurate with those applied to the original design and be approved by the organization that performed the original design unless the applicant designates another responsible organization.</p> <p>10 CFR 73.54(d)(3) requires the licensee to ensure that modifications to assets within the scope of the Rule are evaluated before implementation. 10 CFR 73.54(f) requires the licensee to develop and maintain written policies and implementing procedures to implement the cyber security plan. 10 CFR 73.54(g) requires the licensee to review the cyber security</p>		

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
<p>program as a component of the physical security program in accordance with the requirements of 10 CFR 73.55(m), including the periodicity requirements. Section 4.4.1, "Configuration Management and Change Control," of the [Site/Licensee] Cyber Security Plan states that "CDA [critical digital asset] cyber security and configuration management documentation is updated or created for safety and security systems when such documentation was either unavailable or non-existent (e.g., due to the age of the digital asset, lack of support from the vendor/contractor)." Explain how CDA cyber security and configuration management documentation is updated or created for emergency preparedness and support systems when such documentation was either unavailable or non-existent. Explain which safety-related systems lack current configuration management documentation or have no configuration management documentation.</p>		
<p>11. (37.) 10 CFR 73.54(d)(3) requires the licensee to ensure that modifications to assets within the scope of the Rule are evaluated before implementation. Section 4.4.2, "Cyber Security Impact Analysis of Changes and Environment," of the [Site/Licensee] Cyber Security Plan states "These impact analyses are performed as part of the change approval process to assess the impacts of the changes on the cyber security posture of CDAs and systems that can affect SSEP [safety, security, and emergency preparedness] functions." Explain whether issues identified during these impact analyses are entered into the corrective action program.</p>	<p>NOTE: There are two items marked 11. This item will be designated 11b.</p> <p>Cyber security related issues identified during the change management process are addressed within the change management process, and therefore are not handled by the Corrective Action Program (CAP). Issues identified after the modification is implemented are</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.4.2, Paragraph 3 to read as follows:</p> <p>These impact analyses are performed as part of the change approval process to assess the impacts of the changes on the cyber security posture of CDAs and systems that can affect SSEP functions. Cyber security related issues identified during the change management process are addressed within the change management process, and therefore are not handled by the Corrective Action Program. Adverse conditions identified after the</p>

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
	<p>handled in the CAP.</p> <p>A change to the Plan has been identified to address this concern.</p>	<p>modification is implemented are entered into the site Corrective Action Program.</p>
<p>12. (39.) 10 CFR 73.54(g) requires the licensee to review the cyber security program as a component of the physical security program in accordance with the requirements of 10 CFR 73.55(m), including the periodicity requirements. 10 CFR 73.54(c)(1) requires the licensee to implement security controls to protect the assets identified by paragraph (b)(1) from cyber attacks. Section 4.4.3, "Ongoing Assessment of Cyber Security Controls," of the [Site/Licensee] Cyber Security Plan states "The assessment process verifies the status of these cyber security controls [at least every 24 months] or in accordance with the specific requirements for utilized cyber security controls as described in Appendices D and E of NEI 08-09, Revision 3, whichever is more frequent. For CDAs [critical digital assets] in the site configuration management program, this validation may be performed through a verification of the integrity of the configuration documentation for CDAs." Explain how the effectiveness of each security control is assessed and how the validation process is conducted.</p>	<p>This response answers Draft Generic RAIs 15 and 27, as well.</p> <p>Ongoing assessments are different than reviews.</p> <p>Assessments are:</p> <ul style="list-style-type: none"> • Performed by line organizations • Use INPO 05-05 "Guidance for Performance Improvement." • Cover all areas of the site (e.g. Engineering, Operations, Maintenance, Security, Work Control, Radiological Controls, Chemistry) • Focus on improving performance and looking at Operating Experience, Benchmarking, other assessments • Nuclear licensees have well established performance improvement programs. 	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.4.3 as follows:</p> <p>Delete the following sentence from Section 4.4.3: "For CDAs [critical digital assets] in the site configuration management program, this validation may be performed through a verification of the integrity of the configuration documentation for CDAs."</p>

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
<p>13. (40.) 10 CFR 73.54(b)(2) requires the licensee to establish, implement, and maintain a cyber security program for the protection of the assets within the scope of the Rule. 10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risk. Section 4.4.3.1, "Effectiveness Analysis," of the [Site/Licensee] Cyber Security Plan states "The effectiveness and efficiency of the cyber security program and the cyber security controls in Appendices D and E of NEI 08-09, Revision 3, are monitored to confirm that the cyber security controls are implemented correctly, operating as intended, and achieving the desired outcome." Explain what is meant by "achieving the desired outcome."</p>	<p>The expression, "achieving the desired outcome" is ambiguous. A revision will be made as specified.</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.4.3.1 as follows:</p> <p>Replace: "The effectiveness and efficiency of the cyber security program and the cyber security controls in Appendices D and E of NEI 08-09, Revision 3, are monitored to confirm that the cyber security controls are implemented correctly, operating as intended, and achieving the desired outcome." With "The effectiveness and efficiency of the cyber security program and the cyber security controls in Appendices D and E of NEI 08-09, Revision 3, are monitored to confirm that the cyber security controls are implemented correctly, operating as intended, and continuing to provide high assurance that CDAs are protected against cyber attacks up-to and including the DBT."</p>
<p>14. 10 CFR 73.54(b)(2) requires the licensee to establish, implement, and maintain a cyber security program for the protection of the assets within the scope of the Rule. 10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risk. Section 4.4.3.1, "Effectiveness Analysis," of the [Site/Licensee] Cyber Security Plan states "These measures:</p> <p style="margin-left: 40px;">a. provide insight for improving performance of the Cyber Security Program</p>	<p>Yes, adverse conditions are entered into the Corrective Action Program.</p> <p>A change to the Plan has been identified to address this concern.</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.4.3.1 to include the following as the second-to-last paragraph:</p> <p>Adverse conditions identified during effectiveness evaluations are entered in the site Corrective Action Program.</p>

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
<p>b. assist in determining the effectiveness of cyber security controls in Appendices D and E of NEI 08-09, Revision 3</p> <p>c. assist in ascertaining whether specific cyber security controls are functioning and are helping facilitate corrective action prioritization</p> <p>d. require using the Cyber Security Program activities data with the data obtained from automated monitoring and evaluation tools in a manner that can be tied to cyber security control implementation”</p> <p>Explain whether problems identified during these analyses are entered into the [Site/Licensee] corrective action program.</p>		
<p>15. 10 CFR 73.54(g) requires the licensee to review the cyber security program as a component of the physical security program in accordance with the requirements of 10 CFR 73.55(m), including the periodicity requirements. 10 CFR 73.55(m) states:</p> <p>“Security program reviews. (1) As a minimum the licensee shall review each element of the physical protection program at least every 24 months. Reviews shall be conducted:</p> <p>(i) Within 12 months following initial implementation of the physical protection program or a change to personnel, procedures, equipment, or facilities that potentially could adversely affect security.</p>	<p>NEI 08-09, Appendix A, Section 4.4.3.1 describes the assessment process. The assessment process has been described in the response to RAI 12.</p> <p>Reviews of the cyber security program is described in Section 4.12 which ensures that the periodicity requirements of 10 CFR 73.55(m) are met. The language from 10CFR55(m) is added to Section 4.12 of NEI 08-09 in response to RAI 27.</p>	<p>No change required to NEI 08-09.</p>

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
<p>(ii) As necessary based upon site-specific analyses, assessments, or other performance indicators.</p> <p>(iii) By individuals independent of those personnel responsible for program management and any individual who has direct responsibility for implementing the onsite physical protection program.</p> <p>(2) Reviews of the security program must include, but not be limited to, an audit of the effectiveness of the physical security program, security plans, implementing procedures, cyber security programs, safety/security interface activities, the testing, maintenance, and calibration program, and response commitments by local, State, and Federal law enforcement authorities.</p> <p>(3) The results and recommendations of the onsite physical protection program reviews, management's findings regarding program effectiveness, and any actions taken as a result of recommendations from prior program reviews, must be documented in a report to the licensee's plant manager and to corporate management at least one level higher than that having responsibility for day-to-day plant operation. These reports must be maintained in an auditable form, available for inspection.</p>		

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
<p>(4) Findings from onsite physical protection program reviews must be entered into the site corrective action program."</p> <p>10 CFR 73.54(b)(2) requires the licensee to establish, implement, and maintain a cyber security program for the protection of the assets within the scope of the Rule. 10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risk. Section 4.4.3.1, "Effectiveness Analysis," of the [Site/Licensee] Cyber Security Plan (CSP) states, "The effectiveness of these cyber security controls is verified every 24 months or in accordance with the specific requirements for employed cyber security controls as described in Appendices D and E of NEI 08-09, Revision 3, whichever is more frequent." Explain how the CSP will ensure compliance with the periodicity requirements of 10 CFR 73.55(m).</p>		
<p>16. 10 CFR 73.54(b)(2) requires the licensee to establish, implement, and maintain a cyber security program for the protection of the assets within the scope of the Rule. 10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risk. Section 4.4.3.1, "Effectiveness Analysis," of the [Site/Licensee] Cyber Security Plan describes the monitoring of cyber security controls. Explain the process for review of maintenance and repair records of critical digital asset (CDA) components to ensure that CDAs are maintained according to recommendations provided by the manufacturers and any deviations are justified and</p>	<p>We will incorporate the RG 5.71 text describing this attribute, modified to add the flexibility for sites to modify vendor recommendations to meet site-specific conditions.</p> <p>The term "records" has a specific meaning, and "documents" achieves the same result.</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.4.3.1 as follows:</p> <p>Add the following sentence to the second-to-last paragraph: "Documents of maintenance and repairs on CDA components are reviewed to ensure that CDAs which perform cyber security functions are maintained according to recommendations provided by the manufacturer or as determined by site-specific procedures."</p>

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
documented.		
<p>17. 10 CFR 73.54(b)(2) requires the licensee to establish, implement, and maintain a cyber security program for the protection of the assets within the scope of the Rule. 10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risk. Section 4.4.3.1, "Effectiveness Analysis," of the [Site/Licensee] Cyber Security Plan (CSP) states "The effectiveness criteria are established and the bases documented for established thresholds. The above insights are shared with cyber security decision makers to improve the cyber security at the facility." Describe the effectiveness criteria and thresholds including the bases.</p>	<p>We agree, this is not clear and does not provide value. A modification will be made.</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.4.3.1 as follows:</p> <p>Delete the following sentences: "The effectiveness criteria are established and the bases documented for established thresholds. The above insights are shared with cyber security decision makers to improve the cyber security at the facility."</p>
<p>18. 10 CFR 73.54(b)(2) requires the licensee to establish, implement, and maintain a cyber security program for the protection of the assets within the scope of the Rule. 10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risk. Section 4.4.3.2, "Vulnerability Scans," of the [Site/Licensee] Cyber Security Plan (CSP) states "When new vulnerabilities that could affect the cyber security posture of CDAs [critical digital assets] are identified, testing will be performed on an off-line system where possible and where scanning is deemed necessary." Explain how the off-line test beds or vendor-maintained environments are as realistic as possible.</p>	<p>Through removal of the CDA from service, or replicated in an off-line system or on a vendor test-bed, to the extent feasible.</p> <p>A change to the Plan has been identified to address this concern.</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.4.3.2 as follows:</p> <p>Replace the following sentence: "Where off-line systems, test beds, or vendor maintained environments are used for vulnerability scanning, the systems are configured, where practical, to reproduce the conditions of the operating environment. Where not practical, justification of why the test system configuration is adequate is documented."</p> <p>With "Assessment and scanning process must not adversely impact SSEP functions. If this could</p>

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
		<p>occur, CDAs are removed from service or replicated (to the extent feasible) before assessment and scanning is conducted. If vulnerability assessments or scanning cannot be performed on a production CDA because of the potential for an adverse impact on SSEP functions, alternate controls (e.g., providing a replicated system or CDA to conduct scanning) are employed.”</p>
<p>19. 10 CFR 73.54(e)(2) requires the licensee’s cyber security program to include measures for incident response and recovery for cyber attacks. Section 4.6, “Attack and Mitigation Incident Response,” of the [Site/Licensee] Cyber Security Plan states, “Measures necessary to deny, deter, or detect cyber attacks are implemented by network protective devices and align with the Defensive Strategy.” Security features integrated into critical digital assets (CDAs) can be used to deny, detect, and deter cyber attacks. Explain how these CDA security features will be used to deny, detect, and deter cyber attacks.</p>	<p>CDA security features would be implemented in accordance with Section 3.1.6 or during the ongoing program described in Chapter 4 with respect to addition or modification of assets.</p> <p>A change to the Plan has been identified to address this concern.</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.6.</p> <p>Delete the following Sentence: “Measures necessary to deny, deter, or detect cyber attacks are implemented by [network protective devices] and align with the Defensive Strategy.”</p>
<p>20. 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(e)(2) requires the licensee’s cyber security program to include measures for incident response and recovery from cyber attacks. Section 4.6, “Attack and Mitigation Incident Response,” of the</p>	<p>A change has been identified to remove the reference to “remote” and replace “electronic” with “cyber.”</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.6 to remove the word “remote” and replace “electronic” with “cyber” in the following sentence:</p> <p>“[Policies, Procedures, Programs] document cyber security controls to deny, deter, and detect adverse threats and conditions to CDAs [Critical Digital Assets] that may be</p>

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
<p>[Site/Licensee] Cyber Security Plan (CSP) states “[Policies, Procedures, Programs] document cyber security controls to deny, deter, and detect adverse threats and conditions to CDAs [Critical Digital Assets] that may be susceptible to remote electronic attacks which exploit system vulnerabilities.” Explain how the [Site/Licensee] will deny, deter, and detect threats and conditions to CDAs that may be susceptible to cyber attacks which are not remote (e.g. on-site).</p>		<p>susceptible to remote electronic cyber attacks which exploit system vulnerabilities.”</p>
<p>21. 10 CFR 73.54(e)(2) requires the licensee’s cyber security program to include measures for incident response and recovery for cyber attacks. Section 4.6, “Attack and Mitigation Incident Response,” of the [Site/Licensee] Cyber Security Plan (CSP) states, “Cyber Attacks/Incidents are evaluated, tracked, and managed by the Incident Response and Corrective Action Programs [CAP].” Explain how [Site/Licensee] cyber attacks/incidents will be documented.</p>	<p>A change to the Plan has been identified to address this concern.</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.6 to read as follows:</p> <p>Change the sentence: “Cyber Attacks/Incidents are evaluated, tracked, and managed by the Incident Response and Corrective Action Programs.”</p> <p>To: “Cyber Attacks/Incidents are evaluated, tracked and managed by the Incident Response Program, and any corrective actions resulting from the attacks/incidents are implemented in accordance with the Corrective Action Program.”</p>
<p>22. 10 CFR 73.54(e)(2) requires the licensee’s cyber security program to include measures for incident response and recovery from cyber attacks. Section 4.6, “Attack and Mitigation Incident Response,” of the [Site/Licensee] Cyber Security Plan (CSP) states, “Cyber security attack containment activities are</p>	<p>A change to the Plan has been identified to address this concern.</p> <p>RG 5.71, C-8, states: Assist operations in conducting</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.6.:</p> <p>Change: “Cyber security attack containment activities are directed by site procedures. These</p>

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
<p>directed by site procedures. These measures include but are not limited to:</p> <ul style="list-style-type: none"> a. Isolate the affected CDA [critical digital asset] with approval by [Shift Superintendent Operations], if possible; and b. Verify surrounding networks and support systems are not contaminated." <p>Explain how [Site/Licensee] determines what constitutes "cyber security attack containment activities." Or the criteria used to determine when containment activities are to be instituted.</p>	<p>an operability determination.</p> <p>"Operability determination" has a specific meaning to nuclear operations, and we incorporate the concept as identified.</p> <p>The term "operability" has a nuclear specific meaning (tech specs) – and is applicable to safety systems. We incorporate "functionality" which has the intended effect for non-safety systems.</p>	<p>measures include but are not limited to:</p> <ul style="list-style-type: none"> • Isolate the affected CDA with approval by [Shift Superintendent Operations], if possible; and • Verify surrounding networks and support systems are not contaminated" <p>To: "Cyber security attack containment activities are directed by site procedures. These measures include but are not limited to:</p> <ul style="list-style-type: none"> • Assist in determining the CDA's operability or functionality • Isolate the affected CDA with approval by [Shift Superintendent Operations], if possible; and • Verify surrounding networks and support systems are not contaminated."
<p>23. 10 CFR 73.54(e)(2) requires the licensee's cyber security program to include measures for incident response and recovery from cyber attacks. Section 4.6, "Attack and Mitigation Incident Response," of the [Site/Licensee] Cyber Security Plan states "Recovery activities include but are not limited to functional recovery test, restoration to operational state, verification of operability, and return to service. Systems, networks, and/or equipment affected by cyber attacks are restored and returned to operation as directed by site procedures. Post incident analysis</p>	<p>A change to the Plan has been identified to address this concern.</p> <p>The appropriate location for this modification is in Appendix E, 8.6, "Recovery and Reconstitution."</p> <p>Per discussions with the Staff on February 17, this modification</p>	<p>Revise NEI 08-09, Revision 3, Appendix E, Section 8.6 as follows:</p> <p>In Appendix E, 8.6, "Recovery and Reconstitution" Add the following: "Regression testing is performed before returning to normal operations to ensure that CDA are performing correctly."</p> <p>Revise NEI 08-09, Revision 3, Appendix A,</p>

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
<p>is conducted in accordance with site Corrective Action Program [CAP] procedures.” Explain how the [Site/Licensee] will perform security and requirements testing as part of the recovery activities to ensure the security features are operating properly. Explain how post incident corrective measures ensure that restoration activities do not return the asset to its original, exploitable state. Explain how the [Site/Licensee] ensures that vulnerabilities are not built into the restore point(s).</p>	<p>would address the Staff concerns.</p>	<p>Section 4.6, last paragraph, as follows:</p> <p>Change: “Recovery activities include but are not limited to functional recovery test, restoration to operational state, verification of operability, and return to service. Systems, networks, and/or equipment affected by cyber attacks are restored and returned to operation as directed by site procedures. Post incident analysis is conducted in accordance with site Corrective Action Program procedures.”</p> <p>To: “Recovery activities include but are not limited to functional recovery test, cyber security function and requirements tests, restoration to operational state, verification of operability or functionality, and return to service. Systems, networks, and/or equipment affected by cyber attacks are restored and returned to operation as directed by site procedures. Post incident analysis is conducted in accordance with site Corrective Action Program procedures.”</p>
<p>24. 10 CFR 73.54(e)(2) requires the licensee’s cyber security program to include measures for incident response and recovery from cyber attacks. Section 4.7, “Cyber Security Contingency Plan,” of the</p>	<p>A change to the Plan has been identified to address this concern.</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.7 as follows:</p> <p>Replace:</p>

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
<p>[Site/Licensee] Cyber Security Plan (CSP) provides information about the [Site/Licensee] cyber security contingency plan. Explain how the licensee cyber security contingency plan includes the following:</p> <ul style="list-style-type: none"> a. a formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among [Site/Licensee] entities, and compliance b. formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls <p>Explain the process for [Site/Licensee] updating the contingency planning policy and procedures and, where necessary, related policies and procedures for other programs.</p>	<p>Assessments and reviews are used as the mechanism for updating plans and procedures.</p> <p>The processes used to update contingency planning policy and procedures and, where necessary, related policies and procedures for other programs are the assessment process described in Section 4.4.3, "Ongoing monitoring of Security Controls" and the Cyber Security Program Review process as described in Section 4.12.</p>	<p>"A formal, documented, Cyber Security Contingency Plan protects CDAs from adverse impacts from cyber attack. Refer to Appendix E of NEI 08-09, Revision 3, for additional Cyber Security Contingency Plan cyber security controls."</p> <p>With: "A Cyber Security Contingency Plan protects CDAs from adverse impacts from cyber attack. Refer to Appendix E of NEI 08-09, Revision 6, for additional Cyber Security Contingency Plan cyber security controls.</p> <p>The contingency planning policy is developed, disseminated, periodically reviewed and updated. The contingency planning policy provides the following:</p> <ul style="list-style-type: none"> a. A formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organization entities, and compliance b. Formal, documented procedures to facilitate the implementation of the policy and associated contingency planning controls"
<p>25. 10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risks. Section 4.9,</p>	<p>A change to the Plan has been identified to address this</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.9 as follows:</p>

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
<p>“Evaluate and Manage Cyber Risk,” states “Cyber risk is evaluated and managed utilizing site programs and procedures outlined in the Performance Requirements in Section 2.2. Refer to Appendix E of NEI 08-09, Revision 3, which describes how the following cyber security controls are used to evaluate and manage risk.” The security controls referenced in Section 4.9 are not included in Appendices D and E of NEI 08-09, Rev. 3. Explain how [Site/Licensee] will include these security controls within the appropriate appendix.</p>	<p>concern.</p>	<p>Delete the following sentence: “Refer to Appendix E of NEI 08-09, Revision 3, which describes how the following cyber security controls are used to evaluate and manage risk.”</p>
<p>26. 10 CFR 73.54(d)(1) requires that licensees “[e]nsure that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training necessary to perform their assigned duties and responsibilities.” The [Site/Licensee] Cyber Security Plan (CSP) Section 4.11, Roles and Responsibilities, indicates the Cyber Security Incident Response Team (CSIRT) will respond to a credible cyber attack. Explain how the CSIRT will determine which attacks are credible.</p>	<p>A change to the Plan has been identified to address this concern.</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.11 as follows:</p> <p>In the list introduced “Cyber Security Incident Response Team (CSIRT)”, remove the word “credible” from the last bullet.</p> <p>Delete “credible” from the last bullet, which would read: “Responds to a cyber attack and performs the activities described in Section 4.6. Responsibilities are designated in site [incident/event response] procedures. Ancillary CSIRT staff includes organizations and individuals who operate, maintain, or design critical systems. CSIRT support staff is comprised of organizations and individuals as needed for specific specialized knowledge.”</p>
<p>27. 10 CFR 73.54(g) requires the licensee to review</p>	<p>Security Controls are elements of</p>	<p>Revise NEI 08-09, Revision 3, Appendix A,</p>

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
<p>the cyber security program as a component of the physical security program in accordance with the requirements of 10 CFR 73.55(m), including the periodicity requirements. 10 CFR 73.55(m) states</p> <p style="padding-left: 40px;">“Security program reviews. (1) As a minimum the licensee shall review each element of the physical protection program at least every 24 months. Reviews shall be conducted:</p> <p style="padding-left: 80px;">(i) Within 12 months following initial implementation of the physical protection program or a change to personnel, procedures, equipment, or facilities that potentially could adversely affect security.</p> <p style="padding-left: 80px;">(ii) As necessary based upon site-specific analyses, assessments, or other performance indicators.</p> <p style="padding-left: 80px;">(iii) By individuals independent of those personnel responsible for program management and any individual who has direct responsibility for implementing the onsite physical protection program.</p> <p style="padding-left: 40px;">(2) Reviews of the security program must include, but not be limited to, an audit of the effectiveness of the physical security program, security plans, implementing procedures, cyber security programs, safety/security interface activities, the testing, maintenance, and</p>	<p>the Security Program and are reviewed consistent with the requirements of 10 CFR 73.55(m).</p>	<p>Section 4.12 as follows:</p> <p>Revise 4.12 to add the following wording of the regulation, 10 CFR 73.55(m):</p> <p>“Security program reviews. (1) As a minimum the licensee shall review each element of the physical protection program at least every 24 months. Reviews shall be conducted:</p> <p style="padding-left: 20px;">(i) Within 12 months following initial implementation of the physical protection program or a change to personnel, procedures, equipment, or facilities that potentially could adversely affect security.</p> <p style="padding-left: 20px;">(ii) As necessary based upon site-specific analyses, assessments, or other performance indicators.</p> <p style="padding-left: 20px;">(iii) By individuals independent of those personnel responsible for program management and any individual who has direct responsibility for implementing the onsite physical protection program.</p> <p>(2) Reviews of the security program must include, but not be limited to, an audit of the effectiveness of the physical security program, security plans, implementing procedures, cyber security programs, safety/security interface activities, the testing, maintenance, and calibration program, and response commitments by local, State, and Federal law enforcement authorities.</p> <p>(3) The results and recommendations of the onsite physical protection program reviews,</p>

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
<p>calibration program, and response commitments by local, State, and Federal law enforcement authorities.</p> <p>(3) The results and recommendations of the onsite physical protection program reviews, management's findings regarding program effectiveness, and any actions taken as a result of recommendations from prior program reviews, must be documented in a report to the licensee's plant manager and to corporate management at least one level higher than that having responsibility for day-to-day plant operation. These reports must be maintained in an auditable form, available for inspection.</p> <p>(4) Findings from onsite physical protection program reviews must be entered into the site corrective action program."</p> <p>Section 4.12, "Title," of the [Site/Licensee] Cyber Security Plan (CSP) does not provide an explicit commitment to implement each of the required reviews at the frequency specified in 10 CFR73.55(m). Explain how the review processes required by 10 CFR 73.55(m) including those pertinent to results, recommendations and findings are addressed and committed to within the Cyber Security Program.</p>		<p>management's findings regarding program effectiveness, and any actions taken as a result of recommendations from prior program reviews, must be documented in a report to the licensee's plant manager and to corporate management at least one level higher than that having responsibility for day-to-day plant operation. These reports must be maintained in an auditable form, available for inspection.</p> <p>(4) Findings from onsite physical protection program reviews must be entered into the site corrective action program."</p> <p>Revise 4.12 to add the following: "Security Controls are elements of the Security Program and are reviewed consistent with the requirements of 10 CFR 73.55(m)."</p> <p>Revise NEI 08-09, Revision 3, Appendices D and E as follows: Revise the introductory paragraphs in the Appendices to add: "Security Controls are elements of the Security Program and are reviewed consistent with the requirements of 10 CFR 73.55(m)."</p>
<p>28. 10 CFR 73.54(h) requires the licensee to retain all records and supporting technical documentation required to satisfy the requirements of this section as</p>	<p>A change to the Plan has been identified to address this concern.</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.13 read as follows:</p>

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
<p>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. Section 4.13, "Title," of the [Site/Licensee] Cyber Security Plan (CSP) does not explicitly describe which specific documents [Site/Licensee] intends to use to document access history and use to discover the source of cyber attacks affecting critical digital assets and safety, security and emergency planning functions. Explain how [Site/Licensee] will include this information</p>		<p>4.13 DOCUMENT CONTROL AND RECORDS RETENTION AND HANDLING [Licensor/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.</p> <p>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:</p> <ul style="list-style-type: none"> • 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 <p>The following Audit Records will be retained:</p> <ul style="list-style-type: none"> • Audit Records described in Appendix D, 2.3 • Audit Records that support Appendix

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
		<p>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.</p> <p>Audit (Digital and Non-Digital) Records include:</p> <ul style="list-style-type: none"> o Operating system logs o Service and application logs o Network device logs <p>Audit Record retention duration is determined during the implementation of the program in accordance with Section 3 of this Plan, and will not be less than 90 days. Audit record retention duration may be adjusted based on the results of periodic program effectiveness reviews performed in accordance with Section 4 of this Plan.</p> <p>Individual Cyber Security Training Records will be documented and maintained for 3 Years.</p>
<p>29. 10 CFR 73.54 requires that “Each [Cyber Security Plan] submittal must include a proposed implementation schedule. Implementation of the licensee’s cyber security program must be consistent with the approved schedule.” The implementation schedule provided with the [Site/Licensee] Cyber</p>	<p>This RAI is site-specific; however the Generic RAI Response Team will work with NRC on developing guidance for licensees addressing this site-specific RAI.</p>	<p>No change required to NEI 08-09.</p>

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
<p>Security Plan (CSP) does not appear to be reasonable considering the following:</p> <ul style="list-style-type: none"> a. The NRC 2002 Interim Compensatory Measures Order (EA-02-026), along with the associated implementing guidance, required that [Site/Licensee] identify all of [Site/Licensee]'s digital systems associated with Safety, Security, and Emergency Preparedness (SSEP) and institute appropriate protective measures. b. The NRC 2003 Design Basis Threat (DBT) Order (EA-03-086) added the cyber attack vector to the list of adversary characteristics that [Site/Licensee] must defend against with high assurance. c. The DBT Order also required [Site/Licensee] to revise the site-specific security plans (by 2004) to address all of the new adversary characteristics. d. [Site/Licensee]'s site-specific security plan includes cyber security program provisions for digital assets associated with SSEP functions. e. In 2005 the NRC endorsed the Nuclear Energy Institute's NEI 04-04 "Cyber Security Program for Nuclear Power Plants." It is the understanding of the NRC understanding from discussions with NEI that all power reactor licensees implemented an NEI 04-04 program by 2008. NEI 04-04 described cyber security program provisions for digital assets associated with SSEP functions. 		

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
<p>f. In 2007 the NRC finalized the DBT Rule (10 CFR 73.1) and the associated implementing guidance (Regulatory Guide 5.69) which describe the cyber attack threat. This Rule, in combination with 10 CFR 73.55(b), required power reactor licensees to protect against all DBT adversary characteristics.</p> <p>g. In 2008 NEI and several industry licensees responded to the Federal Energy Regulatory Commission's (FERC) proposed Order 706-B by indicating that FERC's cyber requirements were not needed because NEI 04-04 programs were in place at all power reactor sites.</p> <p>h. The North American Electric Reliability Corporation (NERC) 706-B Implementation Plan requires compliance with the CIP Reliability Standards by the later of the FERC effective date plus 18 months, or the NERC/NRC Memorandum of Understanding execution date plus 10 months. For requirements that are outage-dependent, the NERC Implementation Plan requires compliance with the Critical Infrastructure Protection Reliability Standards within 6 months after the completion of the first refueling outage that is at least 18 months following the FERC effective date.</p> <p>Given the above, justify each date in the CSP implementation schedule provided, including interim milestones.</p>		

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
<p>30. 10 CFR 73.54(c)(1) requires the cyber security program to implement security controls to protect critical digital assets from cyber attacks. Sections 4.4.3.1, "Effectiveness analysis," and 4.4.3.2 "Vulnerability Scans," describe effectiveness analysis and vulnerability scans. Will effectiveness analysis and vulnerability scans be performed at the time security controls are first implemented to provide high assurance they are operating as intended and producing the desired outcome, or only as part of periodic monitoring activities described in Sections 4.4.3.1 and 4.4.3.2?</p>	<p>A change to the Plan has been identified to address this concern.</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, as follows:</p> <p>Revise Section 4.4.3.1, Paragraph 3 to add "when applied, and" so that the sentence will read: The effectiveness of these cyber security controls is verified when applied, and [at least every 24 months] or in accordance with the specific requirements for employed cyber security controls as described in Appendices D and E of NEI 08-09, Revision 3, whichever is more frequent.</p> <p>Revise Section 4.4.3.2, Paragraph 1 to add "when security controls are first applied, and" so that Paragraph 1 will read: Electronic vulnerability scanning of CDAs is performed when security controls are first applied, and as required by specific guidance in the cyber security controls in Appendices D and E of NEI 08-09, Revision 3. When new vulnerabilities that could affect the cyber security posture of CDAs are identified, testing will be performed on an off-line system where possible and where scanning is deemed necessary.</p>
<p>31. 10 CFR 73.54(c)(1) requires the cyber security program to implement security controls to protect critical digital assets from cyber attacks. Section 4.5, "Addition and Modification of Assets" of the Cyber</p>	<p>A change to the Plan has been identified to address this concern.</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.5 as follows:</p> <p>Delete the word "preferred" from Sentence 1,</p>

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
<p>Security Plan (CSP) states that “The preferred approach for assessing new/modified [critical digital assets] CDAs is to use the assessment process described in Section 3.1 of this Plan. Alternately, a process that reviews and addresses Cyber Security Controls listed in Appendices D and E of NEI 08-09, Revision 3, may be used.” Please explain what conditions warrant the use of the alternate assessment process as opposed to those outlined in Section 3.1, and provide greater detail as to how the alternative process mentioned in Section 4.5 provides the same level of assurance as the preferred approach.</p>		<p>and delete Sentence 2: The preferred approach for assessing new/modified CDAs is to use the assessment process described in Section 3.1 of this Plan. Alternately, a process that reviews and addresses Cyber Security Controls listed in Appendices D and E of NEI 08-09, Revision 3, may be used.</p> <p>As the result, Paragraph 1 of section 4.5 would read: The approach for assessing new/modified CDAs is to use the assessment process described in Section 3.1 of this Plan.</p>
<p>32. 10 CFR 73.54(c)(1) requires the cyber security program to implement security controls to protect the assets identified by paragraph (b)(1) of 10 CFR 73.54 from cyber attacks. Section 4.5, “Addition and Modification of Assets,” of the Cyber Security plan (CSP) states, “[Programs, Procedures, Processes] have been established, implemented, and maintained to control life cycle phase activity cyber security controls for [critical digital assets] CDAs. These [programs, procedures, processes] ensure that modifications to a CDA within the scope of 10 CFR 73.54 are evaluated before implementation to ensure that the cyber security performance objectives of 10 CFR 73.54(a)(1) are maintained and that acquired CDAs have cyber security requirements developed to achieve the site’s cyber security program objectives.” This statement addresses acquisition of new CDAs or modifications</p>	<p>Response: Section 4.4.2, “Cyber Security Impact Analysis of Changes and Environment” addresses this concern: “A cyber security impact analysis is performed prior to making a design or configuration change to a CDA, or when changes to the environment occur...”</p> <p>And</p> <p>“These impact analyses are performed as part of the change approval process to assess the impacts of the changes on the</p>	<p>No change needed.</p>

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
<p>made to existing CDAs. Please clarify whether any assets that do not provide direct, or supporting, roles in the proper functioning of critical systems but are later reprogrammed (moved, reconfigured, or modified in any way) for use as a CDA are evaluated before implementation to ensure the security performance objectives of 10 CFR 73.54 are maintained.</p>	<p>cyber security posture of CDAs and systems that can affect SSEP functions.”</p>	
<p>33. 10 CFR 73.54(b)(1) requires the licensee to analyze digital computer and communications systems and networks and identify those assets that must be protected against cyber attacks. Section 2.1 states, “This Plan establishes a means to achieve high assurance that digital computer and communication systems and networks associated with the following functions (hereafter designated as Critical Digital Assets (CDAs)) are adequately protected against cyber attacks up to and including the Design Basis Threat (DBT) as described in § 73.1:</p> <ul style="list-style-type: none"> • Safety-related and important-to safety functions; • Security functions; • Emergency preparedness functions including offsite communications; and • Support systems and equipment which if compromised, would adversely impact safety, security, or emergency preparedness functions.” <p>However, Section 3.1.3 of the CSP of states that “[Critical systems] CSs are identified by conducting an initial consequence analysis of site systems, equipment, communication systems and networks determine those which, if compromised, exploited or</p>	<p>A change to the Plan has been identified to address this concern.</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 3.1.3, Bullet 1 to add a sentence before the parenthesis as described:</p> <p>...nuclear facility without accounting for existing mitigating measures. For those support systems or equipment that are associated with SSEP functions, a dependency and pathway analysis is performed to determine whether those systems or equipment are CSs. (Existing mitigating measures...</p>

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
<p>were to fail, could impact the [Safety, security and emergency preparedness] SSEP functions of the nuclear facility without accounting for existing mitigating measures." Please explain whether the analysis conducted in Section 3.1.3 will include support systems and equipment which if compromised, would adversely impact SSEP functions.</p>		
<p>34. 10 CFR 73.54(b)(1) requires the licensee to analyze digital computer and communications systems and networks and identify those assets that must be protected against cyber attacks. Section 4.4.3.2 states, "Electronic vulnerability scanning of [critical digital assets] CDAs is performed as required by specific guidance in the cyber security controls in Appendices D and E of NEI 08-09, Revision 3. When new vulnerabilities that could affect the cyber security posture of CDAs are identified, testing will be performed on an off-line system where possible and where scanning is deemed necessary." The criteria for when scanning activities will be "deemed necessary" is not clear. Please explain whether the phrase "deemed necessary" applies only to vulnerability scanning performed as part of testing activities. If not, provide the criteria for when electronic vulnerability scans will, and will not be, deemed necessary.</p>	<p>A change to the Plan has been identified to address this concern.</p> <p>Many of the CDA in our plants will not have architectures that are supported by or benefit from scanning. Further, there are no offline systems available for all CDA's and these cannot be procured at any cost at the revision installed. Alternate controls would be used to assess new vulnerabilities and will most likely use the technique originally used to assess the vulnerabilities for that CDA.</p>	<p>Revise NEI 08-09, Revision 3, Appendix A, Section 4.4.3.2 :</p> <p>The relevant Sentence in Section 4.4.3.2 will read: When new vulnerabilities that could affect the cyber security posture of CDAs are identified, vulnerability scanning will be performed on an off-line system, where possible, or via an alternate control that confirms the existence or absence of the new vulnerability at the next system availability window.</p>
<p>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.</p>	<p>A response to this RAI will be submitted to the NRC on or before Wednesday, March 10,</p>	<p>A response to this RAI will be submitted to the NRC on or before Wednesday, March 10, 2010.</p>

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
<p>Section 2.2, "Performance Requirements" provides a list of performance based requirements for the CSP. The following clarifications are needed:</p> <p>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.</p> <p>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.</p> <p>10 CFR 73.54(d)(1) states the licensee shall ensure appropriate facility personnel, including contractors,</p>	<p>2010.</p>	

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
<p>are aware of cyber security requirements and receive 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.</p> <p>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.</p>		