Cyber Security Plan Implementation Schedule

Generic RAI Question # 29 includes reference to previous regulatory guidance and industry initiatives related to cyber security. As referenced, current industry guidance for cyber security is described in NEI 04-04, *Cyber Security Program for Power Reactors*. However, the scope of requirements in the NRC accepted implementation guidance contained in NEI 08-09 revision 6 are significantly greater than the previously implemented cyber security program. The defensive model design requirements, the new digital asset assessment methodology and the resultant digital asset remediation actions will require a significant expenditure of labor resources. As referenced in the Generic RAI Question # 29, [site/fleet] is also required to implement a separate cyber security program in accordance with the NERC Critical Infrastructure Protection Standards. While the timeframe for implementation is shorter for the NERC regulation as described in the RAI question, the NERC cyber security methodology is different from the NRC Rule requirements. The NERC requirements are based on a logical risk based assessment process while the NRC Rule 73.54 requires a deterministic cyber security assessment methodology.

In light of the extensive work associated with implementation of these two new regulations, [site/fleet] has developed a prioritized approach to establish the NRC Rule 73.54 implementation schedule. [Site/Fleet] realizes the importance of deploying a [uni-directional] communication barrier to protect the most critical SSEP functions. One major activity is the deployment of [uni-directional] communication barrier to ensure protection from remote attacks on plant systems. While the deployment of the [uni-directional] barrier is critical to protection from external cyber threats, it also impacts remote access to plant data systems by authorized personnel. This elimination of remote access will require Licensees to develop and implement a detailed change management plan.

Another major activity is the performance of individual critical digital asset (CDA) assessments to identify individual asset security control remediation actions. Programs and procedures are being developed to implement the programmatic requirements of the regulation. The cyber security assessment teams are also being established for execution of program requirements. These teams are required to have extensive knowledge of plant systems and cyber security control technology. A comprehensive training program will be required to ensure competent personnel for program execution.

Following are the Cyber Security implementation milestones that have been developed based on the sample listing of milestones provided with your December 2009 implementation schedule guidance:

Implementation Milestone	Completion Date	Basis
Train and Qualify Cyber Security Assessment Team (CSAT)	[6/2011]	The CSAT will require a broad and very specialized knowledge of information and digital systems technology. The CSAT will need to have digital plant systems knowledge as well as nuclear power plant operations, engineering and nuclear safety experience and technical expertise. The personnel selected for this team will require additional training in these areas to ensure adequate capabilities to meet the regulation requirements. By the completion date, the following will be performed: • Cyber security assessment procedures/tools will be developed and available; • Qualifications for CSAT will be developed; and • Training of the CSAT will be completed.
Identify Critical Systems (CSs) and Critical Digital Assets (CDAs)	[6/2011]	By the completion date, the following will be performed: • Critical Systems will be identified; and • Critical Digital Assets will be identified.
Develop Cyber Security Defensive Strategy (i.e., defensive model)	[6/2011]	The Defensive Strategy expands upon the high level model in the Cyber Security Plan and requires assessment of existing site and corporate policies, comparison to new requirements, revisions as required, and communication to plant personnel. By the completion date, the following will be performed: • Documenting the defense-in-depth architecture and defensive strategy; • Revisions to existing defensive strategy policies will be implemented and communicated; and • Planning the implementation of the defense-in-depth architecture.
Implement cyber security defense-in-depth architecture	[6/2012 – for isolation boundaries] [6/2013 – for other boundaries]	The implementation of communication barriers protects the most critical SSEP functions from remote attacks on our plant systems. While the deployment of the barriers is critical to protection from external cyber threats, it also prevents remote access to core monitoring and plant data systems for reactor engineers and other plant staff. This elimination of remote access to core monitoring systems requires the development and execution of a detailed change management plan to ensure continued safe operation of the plants.

Implementation Milestone	Completion Date	Basis
		Vendors may be required to develop software revisions to support the model. The modification will be developed, prioritized and scheduled. Since software must be updated on and data retrieved from isolated systems, a method of patching, updating and scanning isolated devices will be developed. By the completion date, the following will be performed: • Installation of [deterministic one-way] devices to implement defensive layer boundaries.
Establish Cyber Security Program policies/procedures	[12/2013]	The implementation of the cyber security program is expected to require policy/procedure development and/or upgrades for nearly every plant department. The procedural development for the cyber security program requirements and all of the individual security controls will be far-reaching. Many of the security controls will require development of the technical processes for implementing the control in a nuclear plan environment including development of new procedures for surveillances, periodic monitoring and reviews. Procedure development will begin early in the implementation of the program and continue until the specified completion date. By the completion date, the following will be performed: • Policies/procedures will be updated to establish Cyber Security Program ; • The Cyber Security Assessment Procedure will be issued; and • New policies/procedures or revision of existing policies/procedures in areas impacted by cyber security requirements will be develop and implemented.
Perform and document the cyber security assessment described in the Cyber Security Plan	[12/2013]	Based on the existing cyber security program, it is known that the number of digital assets requiring assessment is extensive. . As previously discussed, the CDA assessment methodology required for this regulation is extremely rigorous and deterministic. The completion of these assessments will require a significant commitment of resources. The assessments will not begin prior to having a fully established CSAT and the required procedures. Performing the assessments will require participation of multiple disciplines and involve document reviews, system configuration evaluation, physical walk downs or electronic verification of every communication pathway for each CDA, and documentation of results. These tasks will need to be coordinated and scheduled to align with department resource availability and system access requirements.

Implementation Milestone	Completion Date	Basis
		By the completion date, the following will be performed: • Cyber security assessments will be performed and documented.
Implement Security Controls not requiring a plant modification. The Cyber Security Program is implemented and the Program has entered maintenance phase.	[4 years after NRC approval of Cyber Security Plan]	Although the scope of individual CDA assessment remediation actions is unknown, based on the number and complexity of the required security controls, it is expected to be a significant effort. Each of the individual CDA remediation actions will need to be planned, resourced, and executed. This date is only a commitment for the remediation actions not requiring a plant modification. Changes requiring a plant modification may be implemented during the ongoing maintenance of the cyber security program. A rigorous planning process is used to ensure safe execution of refueling outage work. The potential system modifications required by this regulation need to be carefully planned and executed to ensure no detrimental effect to safe plant operations. The Program will be considered implemented and transitioned to the maintenance phase if modifications have either been implemented, or are budgeted and scheduled for implementation. By the completion date, the following will be performed: • Security controls (that do not require plant modification) will be implemented in accordance with Section 3.1.6 of the Plan. The application of security controls requiring plant modifications will be planned, budgeted, and scheduled. Beginning on this date, during the ongoing maintenance of the Program, the following will be included: • The requirements of Section 4 of the Plan will be effective; and • Implementing plant modifications, per the schedule developed above, that have not been completed.