Cyber Security Plan Implementation Schedule

Title 10 of the Code of Federal Regulations, Part 73, “Physical Protection of Plants and Materials,” Section 73.54, “Protection of Digital Computer and Communication Systems and Networks,” requires licensees 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. As required by 10 CFR 73.54 (b)(3) the cyber security program is a component of the physical protection program. The physical protection and cyber security programs are mutually supportive of the goal of preventing acts of radiological sabotage. The physical protection program currently in place, including the access authorization program and insider mitigation program, supports the protection of plant equipment from unauthorized access by an un-trusted individual. The insider mitigation program critical group has been expanded to include addressing cyber security staff in accordance with RG 5.77, and was completed by March 31, 2010. This action in combination with the other elements of insider mitigation program supports addressing the insider threat. The critical group of the Insider Mitigation Program includes: any individual who has the combination of electronic access and the administrative control (e.g., “system administrator" rights) to alter one or more security controls associated with one or more critical digital assets; and any individual with extensive knowledge of the site-specific cyber defensive strategy.

Ensuring physical protection is a fundamental driver of cyber security by eliminating threat vectors associated with direct physical access. The deployment of a [deterministic isolation] communication barrier ensures protection from remote attacks on plant systems. While the deployment of the [deterministic isolation] 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. [Site/Fleet] also recognizes the threats associated with portable media (e.g., USB thumb drives, CDs, etc.) and portable equipment (e.g., laptops) that connect to un-trusted networks. Cyber security management, operational, and technical controls to address portable media and equipment will be implemented early in the program. A common control is a security control that, once fully implemented, provides cyber security protection to one or more Critical Digital Assets (CDA) or Critical Systems (CS). The protections provided by a common security control can be inherited by CDAs and CSs throughout the facility. Therefore, the establishment of common controls will be prioritized in the implementation of the Cyber Security Program.

Target sets are protected commensurate with their impact on safety. Target set equipment or elements are contained within a protected or vital area or are identified and documented consistent with the requirements in §73.55(f)(1) and accounted for in the [licensee's] protective strategy. The site physical protection program provides high assurance that these elements are protected from physical harm by an adversary. The consideration of cyber attack during the development of target sets is performed in accordance with 10 CFR 73.55 (f)(2). The cyber security program will enhance the defense-in-depth nature of the protection of CDAs associated with target sets.

A final date by which all management, operational, and technical cyber security controls will be implemented for CDAs is provided within the [Licensee] proposed Implementation Schedule. The priority implementation of key aspects of the cyber security program will be accomplished by establishing the following elements, as described in the schedule below, by December 31, 2012: [

- Deterministic isolation, as described in Section 4.3, “Defense-In-Depth Protective Strategies” of the Cyber Security Plan, will be in place;
- The training of staff and the implementing steps to add signs of cyber security-related tampering to insider mitigation rounds will be complete;
- Implementation of the management, operational, and technical cyber security controls that address attacks promulgated by use of portable media, portable devices, and portable equipment will be complete;
- As a parallel activity to the above, [the Licensee] will identify, document, and implement common controls from those controls listed in the Cyber Security Plan, and outstanding CDA-specific modifications associated with the implementation of site common controls not complete by 12/31/2012 will be documented in the site configuration management and/or change control program; and,
- Ongoing monitoring and assessment activities will commence, as described in Section 4.4, “Ongoing Monitoring and Assessment” of the Cyber Security Plan, for those CDAs whose security controls have been implemented.

]

Full implementation of the cyber security program involves many supporting tasks. Major activities include: program and procedure development; performing of individual critical digital asset (CDA) assessments; and identification, scheduling, and implementing individual asset security control remediation actions through the site configuration management program. 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.

The configuration management program specifies a modification process governed by engineering design control. The plant modification process is used for design and configuration changes to CDAs. The plant modification process plans, analyzes, budgets, designs, evaluates risk, implements, installs, and tests configuration changes to CDAs. Some plant modifications to CDAs may be done while the plant is operational. Changes to CDAs whose function supports safety or operational requirements (e.g., safety, surveillance tests, operational decisions, technical specification requirements, security) must be scheduled and performed outside the normal day-to-day operation of the CDA. Based on the complexity of the modification and potential impact to the site, the modification may take 18 to 24 months to fully implement. This time duration ensures the modification is scheduled and performed at a time that minimizes impact to plant safety and operations, up-to and including the need for scheduling the modification during a scheduled plant refueling outage.

The following Cyber Security Program implementation milestones apply:

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]	This milestone builds on work done to identify critical assets under NEI 04-04. The scope of 10 CFR 73.54 expands the scope of NEI 04-04, and therefore, a truing up of the identification of critical assets will be performed. By the completion date, the following will be performed:

Implementation Milestone	Completion Date	Basis
		• 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. Isolating the plant control systems from the Internet as well as from the corporate business systems is an important milestone in defending against external threats. [Recognizing the threat vectors associated with electronic access, the installation of hardware-based deterministic isolation devices will be prioritized.] 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 reactor core monitoring systems requires the development and execution of a detailed change management plan to ensure continued safe operation of the plants. 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.

Implementation Milestone	Completion Date	Basis
		By the completion date, the following will be performed: • Installation of [deterministic one-way] devices to implement defensive layer boundaries. By 12/31/2012, the following element of this milestone will be complete: • Implementation of the management, operational, and technical cyber security controls that address attacks promulgated by use of portable media, portable devices, and portable equipment will be complete.
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. The development and modification of associated policies and procedures will be performed in a risk-informed process, supporting the addressing of security controls as identified during the assessment. 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; By 12/31/2012, the following elements of this milestone will be complete: • Common controls are identified, documented, and implemented, and

Implementation Milestone	Completion Date	Basis
		outstanding CDA-specific modifications associated with the implementation of site common controls not complete by 12/31/2012 are documented in the site configuration management and/or change control program (to include planned implementation dates for these CDA-specific modifications); and • The training of staff and the implementing steps to add signs of cyber security-related tampering to insider mitigation rounds will be complete.
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. 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	[DATE, not contingent on the approval of the 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.

Implementation Milestone	Completion Date	Basis
maintenance phase.		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.
Implement security controls requiring a plant modification.	[DATE]	By this date, if there are outstanding modifications or controls that required a scheduled plant refueling outage to complete, then these associated: • Modifications are implemented; • Procedures are updated; and • Training completed. By this date, all management, operational, and technical security controls will be implemented for CDAs