

Guidance on Cyber Security Plan Implementation Schedule

Cyber Security Plan Implementation Schedule

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 design remediation actions through the site configuration management program. These design modifications may be performed on-line or could require a refueling outage for installation.

The extensive workload associated with full implementation of the Cyber Security Plan (CSP) requires prioritization to assure those activities that provide higher degrees of protection against radiological sabotage are performed first. Therefore the CSP implementation schedule will be implemented with two major milestone dates. The first milestone date of no later than December 31, 2012, includes the activities listed in the table below. The second milestone date, [XXXXXX, XX, XXXX], includes the completion of all remaining actions that result in the full implementation of the cyber security plan for all applicable Safety, Security, and Emergency Preparedness (SSEP) functions. This date also bounds the completion of all individual asset security control design remediation actions.

Cyber security controls are not applied if the control adversely impacts safety and important to safety, security or emergency preparedness functions.

#	Implementation Milestone	Completion Date	Basis
1	Establish Cyber Security Assessment Team (CSAT) as described in Section 3.1.2 "Cyber Security Assessment Team" of the Cyber Security Plan (CSP).	No later than December 31, 2012	The CSAT, collectively, 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 may require additional training in these areas help to ensure adequate capabilities to perform cyber security assessments as well as others duties.
2	Identify Critical Systems (CSs) and Critical Digital Assets (CDAs) as described in Section 3.1.3 "Identification of Critical Digital Assets" of the CSP.	No later than December 31, 2012	The scope of 10 CFR 73.54 includes digital computer and communication systems and networks associated with: 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. The scope of 10 CFR 73.54 includes structures, systems, and components (SSCs) that have a nexus to radiological health and safety and therefore can directly or indirectly affect reactivity of a nuclear power plant and could

Guidance on Cyber Security Plan Implementation Schedule

#	Implementation Milestone	Completion Date	Basis
			result in an unplanned reactor shutdown or transient.
3	<p>Implement Installation of a [deterministic one-way] device between lower level devices ([level 0 1,2]) and the higher level devices ([level 3,4]) as described in Section 4.3, "Defense-In-Depth Protective Strategies" of the CSP.</p> <p>Lower security level devices ([level 0, 1, 2 devices]) that bypass the deterministic device and connect to level 3 or 4 will be modified to prevent the digital connectivity to the higher level or will be modified to meet cyber security requirements commensurate with the level [3 or 4] devices to which they connect.</p> <p>The design modifications that are not finished by the completion date will be documented in the site configuration management and/or change control program to assure completion of the design modification as soon as possible, but no later than the final implementation date.</p>	No later than December 31, 2012	The implementation of communication barriers protects the most critical SSEP functions from remote attacks on plant systems. Isolating the plant systems from the internet as well as from the corporate business systems is an important milestone in defending against external threats. 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, plant operations, and other plant staff. This elimination of remote access to reactor core monitoring systems may require 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.
4	The security control "Access Control For Portable And Mobile Devices" described in Appendix D 1.19 of NEI 08-09, Revision 6, will be implemented.	No later than December 31, 2012	Portable media devices are used to transfer electronic information (e.g., data, software, firmware, virus engine updates and configuration information) to and from plant process equipment. Careful use of this class of media is required to minimize the spread of malicious software to plant process equipment. The effective implementation of this control may require the coordinated implementation of other complimentary controls to ensure adequate mitigation.
5	Implement observation and identification of obvious cyber related tampering to existing insider mitigation	No later than December 31, 2012	Insider mitigation rounds by trained staff look for obvious signs of cyber related tampering and would provide mitigation of observable cyber

Guidance on Cyber Security Plan Implementation Schedule

#	Implementation Milestone	Completion Date	Basis
	rounds by incorporating the appropriate elements in Appendix E Section 4.3 "Personnel Performing Maintenance And Testing Activities."		related insider actions. Implementing steps to add signs of cyber security-related tampering to insider mitigation rounds will be performed by the completion date.
6	<p>Identify, document, and implement cyber security controls in accordance with the Cyber Security Plan Section 3.1.6 "Mitigation of Vulnerabilities and Application of Cyber Security Controls" for CDAs that could adversely impact the design function of physical security target set equipment.</p> <p>The implementation of controls that require a design modification that are not finished by the completion date will be documented in the site configuration management and/or change control program to assure completion of the design modification as soon as possible, but no later than the final implementation date.</p>	No later than December 31, 2012	The site physical protection program provides high assurance that these elements are protected from physical harm by an adversary. The cyber security program will enhance the defense-in-depth nature of the protection of CDAs associated with target sets. Implementing Cyber Security Plan security controls to target set CDAs provides a high degree of protection against a cyber related attacks that could lead to radiological sabotage. Security controls will be addressed in accordance with Cyber Security Plan Section 3.1.6 with the exception of those that require a design modification.
7	Ongoing monitoring and assessment activities commence, as described in Section 4.4, "Ongoing Monitoring and Assessment" of the CSP, for those target set CDAs whose security controls have been implemented.	No later than December 31, 2012	The ongoing monitoring and assessment activities as described in Section 4.4, "Ongoing Monitoring and Assessment" of the Cyber Security Plan will be implemented for the controls applied to target set CDAs. This action results in the commencement of the cyber security program for target set related CDAs.
8	Full implementation of [the Licensee] Cyber Security Plan for all SSEP functions will be achieved.	[XXXX, XX, XXXX]	By the completion date, [the Licensee] Cyber Security Plan will be fully implemented for all SSEP functions in accordance with 10 CFR 73.54. This date also bounds the completion of all individual asset security control design remediation actions including those that require a refuel outage for implementation.