Appendix A: Description of Milestones 1 – 8 of 10 CFR 73.54 Implementation

Due to a variety of valid site-specific operational and technical issues, full implementation dates for Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54, "Protection of digital computer and communication systems and networks," varied significantly among the operating fleet. With such a wide range, the NRC staff worked with the nuclear industry to develop 7 interim implementation milestones to ensure an acceptable level of protection against cyber security threats at each nuclear power reactor until full implementation (now called Milestone 8) 10 CFR 73.54 is achieved.

In its NRC-approved implementation schedule, each licensee committed to meet these 7 interim milestones by December 31, 2012. The 8th Milestone is full implementation. The 8 Milestones are as follows:

1. Establishment of a Cyber Security Assessment Team.
   - This requires formation of a team that has the responsibility to oversee the implementation of the Cyber Security Program and should include personnel from Operations, Security, Engineering, Information Technology, Digital Instrumentation and Controls, and Emergency Preparedness.
2. Identification and documentation of critical systems (CSs) and critical digital assets (CDAs) safety, security, and emergency preparedness using an acceptable or recognized approach per 10 CFR 73.54.
   - This requires all CDAs that perform safety, important to safety, security, and emergency preparedness be identified using an acceptable or recognized approach per 10 CFR 73.54.
3. Installation of protective devices between lower and higher security levels.
   - This requires installation of protective devices (either firewalls or deterministic diodes) that prohibit or restrict communication between lower security levels and higher security levels.
4. Implementation of access control for portable media devices.
   - This requires administrative and technical controls for the protection of thumb drives, laptops and portable equipment used for maintenance and testing of CDAs.
5. Observation for, and identification of, cyber security tampering.
   - This requires protecting CDAs from tampering. This could include monitoring of equipment by security on insider mitigation rounds, installation of tamper tape, and observation of individuals under the Insider Mitigation Program.
6. Implementation of cyber security controls for CDAs that could adversely impact the design function of critical safety equipment.
   - This requires a small set of critical plant equipment to have various cyber security controls implemented to ensure that those assets were protected.
7. Implementing and commencing on-going monitor and assessment activities.
   - This requires that a small set of critical plant equipment to be monitored and assessed to ensure that the cyber security controls were effectively implemented.
8. Full implementation of the Cyber Security Rule (10 CFR 73.54).
   - This requires all of the controls required by the licensees' cyber security plan to be implemented. Most licensees committed to implement the approximately 147 controls required by the Nuclear Energy Institute's 08-09, Rev. 6 for their CS and CDAs. Since licensees have identified hundreds, if not thousands, of CDAs, implementing the controls for all of these assets has been a significant undertaking.