

U.S. NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

US Views on Cyber Threat Assessment and Cyber DBT Development

August 18, 2015

- **Following the events of September 11, 2001, the NRC underwent a comprehensive review of the security requirements and potential vulnerabilities at regulated nuclear facilities**
 - The NRC issued security orders to quickly impose requirements to enhance security above what was already required by existing regulations
 - This included the consideration of cyber security
 - Orders issued in 2002 and 2003 contained requirements for licensees to implement interim compensatory measures
 - Included measures for both physical and cyber-based security
 - Added “cyber-based attacks” as a characteristic of the design basis threat

- **In 2009, the NRC issued new cyber security regulation (10 CFR 73.54) for nuclear power reactors**
 - The cyber security regulation requires the licensee’s cyber security program to be incorporated as a **component of the physical protection program**
 - The cyber security plan is one of four security plans described in 10 CFR 73.55, “Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage”:
 - Physical Security Plan
 - i.e., how a facility establishes and maintains their on-site security organization
 - Training and Qualification Plan
 - i.e., how a facility trains and qualifies security personnel
 - Safeguards Contingency Plan
 - i.e., how a facility implements predetermined response plans and strategies
 - Cyber Security Plan
 - i.e., how a facility protects Critical Digital Assets (CDAs) from cyber-based attacks

- **The DBT is codified in Title 10 of the Code of Federal Regulations, Part 73.1 (10 CFR 73.1)**
 - Licensees are required to protect against:
 - Radiological sabotage
 - Theft or diversion of formula quantities of strategic special nuclear material

Both categories specifically list "Cyber Attack" as an attack vector to be defended against

- **10 CFR 73.54 requires licensees to:**
 - Provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks
 - To a level up to and including the DBT as described in 10 CFR 73.1
 - Protect digital computer and communication systems and networks associated with:
 - Safety-related and important-to-safety functions
 - Security functions
 - Emergency preparedness functions
 - Including offsite communications
 - Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions

- **10 CFR 73.54 requires licensees to protect the systems and networks within the aforementioned scope from cyber attacks that would:**
 - Adversely impact the **integrity** or **confidentiality** of data and/or software
 - **Deny access** to systems, services, and/or data
 - **Adversely impact the operation** of systems, networks, and associated equipment

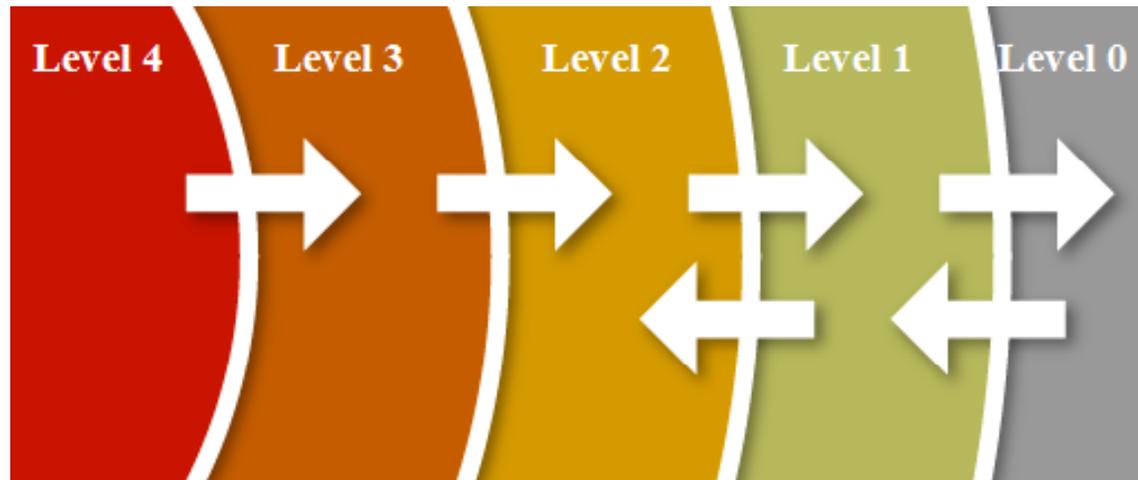
Cyber Security Regulation: Required Actions

- **Per 10 CFR 73.54, the licensee is required to:**
 - Analyze digital computer and communication systems and networks and identify those assets that must be protected against cyber attacks
 - Establish, implement, and maintain a cyber security program for the protection of identified assets
 - **Incorporate the cyber security program as a component of the physical protection program**

- **Regulatory Guide (RG) 5.71 provides guidance on an acceptable approach to satisfy the requirements of 10 CFR 73.54**
 - RG 5.71 also promotes the use of a **multi-level defensive strategy** and outlines other important considerations that should be part of a comprehensive cyber security program
 - Appendix A of RG 5.71 includes a cyber security plan template that applicants and licensees can use and modify as necessary to account for site specific conditions
 - Appendix B and C of RG 5.71 provide details of technical and operational security controls that should be considered in the Cyber Security Plan

- **10 CFR 73.54 requires the use of defense-in-depth strategies to protect CDAs from cyber attacks up to and including the DBT**
- **RG 5.71 recommends the incorporation of a defensive architecture that establishes formal communication boundaries (e.g., security levels)**
 - This may be accomplished via a series of concentric defensive levels of increasing security
 - This is **similar to, and may even correspond with, existing physical security areas** at a facility
 - e.g., vital area, protected area, owner-controlled area, corporate accessible area, public area

Cyber Security Guidance: Defensive Architecture Example



- CDAs associated with safety, important to safety and security functions are allocated to Level 4 and are protected from all lower levels
- **Only one-way data flow is allowed from Level 4 to Level 3 and from Level 3 to Level 2**
- **Communication to a given Security Level may not be initiated at a lower security level**
- Data only flows from one level to other levels through a device or devices that enforce security policy between each level
- **Communication between CDAs at the same Security Level is permitted**

Implementation of Cyber Rule: Phased Implementation

- **Implementation of the operating power reactor cyber security plans are divided into two phases:**
 - Milestones 1-7
 - **Addresses key threat vectors**
 - Completed at all power reactors on December 31, 2012
 - NRC inspection staff is in the process of verifying implementation.
 - Milestone 8
 - **Full cyber security program implementation**
 - Power Reactor licensees are currently in the process of implementing this milestone

Implementation of Cyber Rule: Consequence-Based Approach

- Worked with industry to endorse a consequence-based process to allow a graded approach to assessment of Critical Digital Assets (CDAs).
- **Consequence screening process to enable licensees to screen low consequence CDAs and credit existing programs in lieu of additional cyber security controls and analysis**
- **CDAs that directly impact a Safety, Security and Emergency Preparedness (SSEP) function require full analysis as discussed in Regulatory Guide 5.71**
- Balance of Plant systems require at minimum equivalent protection to NERC Critical Infrastructure Protection standards
- Low consequence CDAs need controls to ensure:
 - Redundant means to detect CDA compromise
 - Adequate time to detect, assess and respond
 - Procedures, equipment and training in place to mitigate the cyber event
 - Common Milestone 1-7 controls

-
- **The DBT considers Cyber Security to be an element of Nuclear Security**
 - **The NRC's Cyber Security rule utilizes a programmatic approach**
 - **Regulatory Guidance recommends a cyber security defensive architecture that, at a high level, is similar to the physical security architecture**

- **10 CFR Part 73, “Physical Protection of Plants and Materials,” U.S. Nuclear Regulatory Commission, Washington, DC**
- **Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities,” U.S. Nuclear Regulatory Commission**
- **NUREG/CR-7141, “The U.S. Nuclear Regulatory Commission’s Cyber Security Regulatory Framework for Nuclear Power Reactors,” November 2014**
- **Regulatory Information Conference (RIC) 2014, “Current Status of Cyber Security Implementation”**