NRC Cyber Security Regulatory Overview

State Liaison Officers Conference
September 26, 2017
Rockville, Maryland

James Beardsley, Cyber Security Branch Chief
Division of Physical and Cyber Security Policy (DPCP)
Office of Nuclear Security and Incident Response (NSIR)

Background

Power Reactor Cyber Security History

- **2002-2003:** NRC included the first cyber requirements in Physical Security and Design Basis Threat Orders
- **2005:** NRC supported industry voluntary cyber program (NEI 04-04)
- **2009:** 10 CFR 73.54, Cyber Security Rule
- **2012:** Implementation/Oversight of Interim Cyber Security Milestones
- **2013-2015:** Milestone 1-7 Inspections
- **2015:** 10 CFR 73.77, Cyber Security Notification Rule
- **2017**: Full Cyber Security Implementation

Regulatory Guide 5.71 Conceptual Approach

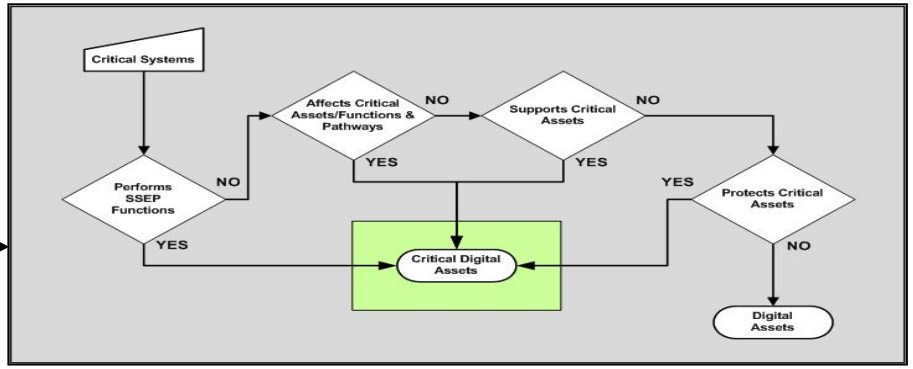
Cyber Security Assessment Team

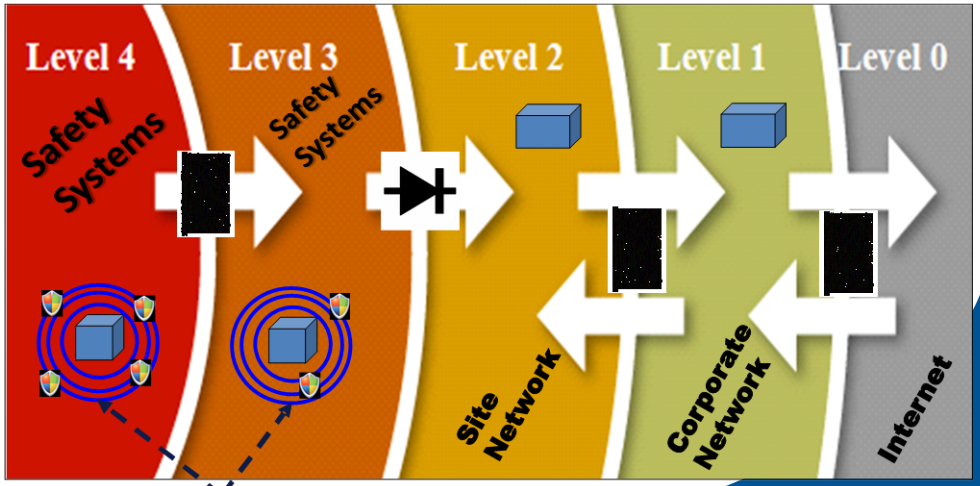
Identify Critical Digital Assets

Apply Defensive Architecture

Address Security Controls

1. Address each control for all CDAs, or
2. Apply alternative measures, or
3. Explain why a control is N/A





Security Systems Level 4 or Level 3 or a separate air gapped network

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Interim Milestones

- Establish Multi-disciplinary Cyber Assessment Team
- Identify Critical Digital Assets
- Establish Defensive Architecture- Isolation of the Most Critical Assets
- Control Portable Media and Devices
- Enhanced Insider Mitigation
- Controls Established for Most Significant Components
- Ongoing Monitoring and Assessment of controls

IMPLEMENTED BY DECEMBER 2012

Power Reactors & COL Holders

- Milestone 1-7 Inspections Conducted 2013-2015.
- Milestone 8 (Full Cyber Implementation) Complete no later than December 2017
- Full Implementation Inspections 2017-2020
  - The NRC and Licensees have learned a lot of lessons through the implementation process.
  - Graded approach to CDA control application through NEI 13-10.

Full Implementation Details

- Expands scope to include all Critical Digital Assets (CDAs)
  - All Safety & Security – Full Cyber Controls
  - Graded Approach for Important-to-Safety, Emergency Preparedness (EP) & Balance-of-Plant (BoP)
    - Some Important-to-Safety, the EP and BoP CDAs are evaluated as Non-Direct
    - Non-Direct CDAs have a minimal set of controls applied

Full Implementation - Cyber Programs

- Attack Mitigation and Incident Response Testing and Drills
- Continuity of Operations Training, Testing
- Secure Communication Pathways to CDAs
  - Ensure only authorized, protected communication from known devices is permitted
- Supply Chain
  - Adds security requirements relevant to vendors, contractors, and developers
- Ensure Availability and Integrity of Information To, From, and On CDAs
  - Prevent CDAs from accessing, receiving, transmitting, or producing unverified or untrusted information
- Configuration Management
- Ongoing Evaluation and Management of Cyber Risk
- Audit and Accountability
  - Validates effectiveness of the cyber security program and controls

Cyber Security Notification

- The Cyber Security Notification Rule, 10 CFR 73.77 became effective on December 2, 2015
- Implementation date – May 2, 2016
- Regulatory Guide 5.83 provides NRC guidance
- NEI guidance document (NEI 15-09)

Other NRC Cyber Initiatives

- Fuel Cycle Facilities
  - Cyber Security Rulemaking in Progress
  - Lessons learned from power reactor implementation
- Non Power Reactors
  - Best Practices Guidance
- Independent Spent Fuel Storage Installations
  - No cyber requirement, may re-evaluate in the future.
- Nuclear Materials
  - Under evaluation by the NRC staff
- Decommissioning
  - Plant planning to decommission may be given relief on full implementation

Questions

10 CFR 73.54 Requirements

1. Identify Critical Digital Assets (CDAs).
2. Apply & Maintain a Defense-in-Depth Protective Strategy.
3. Address Security Controls for each CDA.
4. Identify, Respond and Mitigate against cyber attacks.
5. Training commensurate with roles and responsibilities to facility personnel.
6. Review/Maintain the CSP as a component of the Physical Security Plan.
7. Retain records and supporting technical documentation.

Preparation for Full Implementation

- Addressed SFAQs
- Conducted tabletop exercises with licensees
- Updated cyber security plans (NEI 08-09) and NEI 13-10
- Developed inspection procedures