

# **Nuclear Regulatory Commission**

## **Cyber Security Program Implementation Updated for ACRS**

**Scott Shaeffer, Branch Chief, RII/DRS/EB2**  
**July 28, 2016**

## **Briefing Topics to be Discussed**

- NRC Cyber Security History
- Guidance Documents
- Completed Milestone 1-7 Interim Cyber Security Program Attributes
- Milestone 8 Full Implementation
- Cyber Reporting Requirements
- Other Cyber Related Topics

## Limitations for Cyber Discussions

- Most Cyber Security reports and other information are security related (not Public)
- Unique Cyber Security Language
  - Critical Digital Assets (CDAs), threat vectors, digital controls, portable media controls, etc.

# NRC Cyber Security History

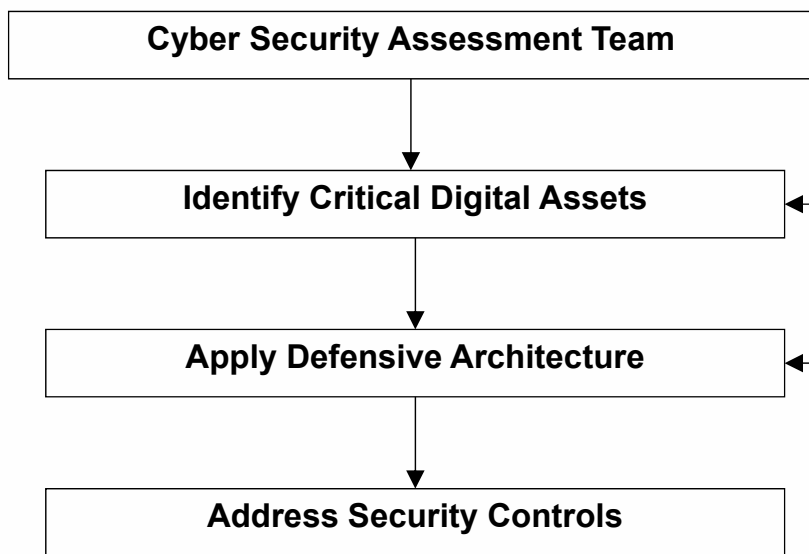


- **2002-2003:** NRC included the first cyber requirements in Physical Security and Design Basis Threat Orders
- **2005:** NRC supported industry voluntary cyber program (NEI 04-04)
- **2009:** 10 CFR 73.54, Cyber Security Rule
- **2010:** NRC published Regulatory Guide 5.71
- **2012:** Implementation of Interim Cyber Security measures
- **2014-2015:** Endorsed NEI 13-10 Cyber Security Control Assessments
  - Graded Consequence Based Approach
- **December 2015** – Completed initial cyber inspections at all Part 50 reactors

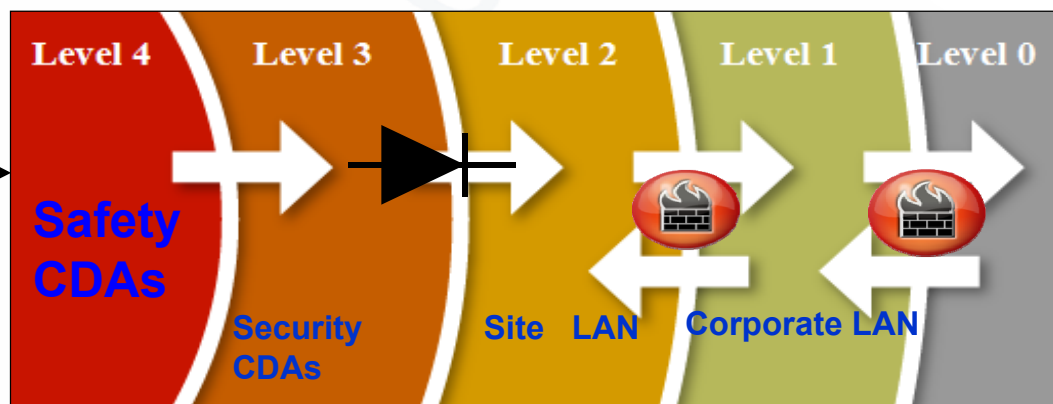
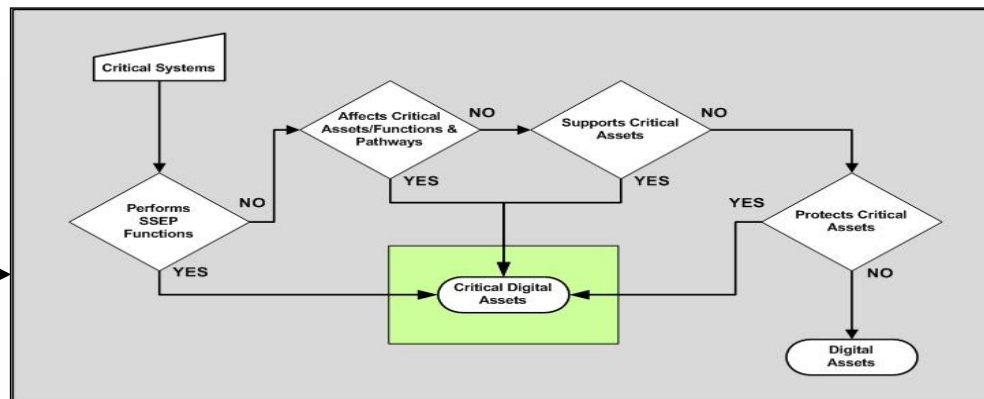
## Guidance Documents for Cyber Implementation

- Regulatory Guide (RG) 5.71 “**Cyber Security Programs for Nuclear Facilities**” (Jan 2010)
- NEI 08-09, Rev. 6 “**Cyber Security Plan For Power Reactors**” (April 2010)
- NEI 13-10, Rev 4 “**Cyber Security Assessments**” (December 2015)

# RG 5.71 Conceptual Approach



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





## Milestones 1-7 Interim Implementation

- Required controls for key CDAs by 12/31/2012
- Initial NRC inspections completed 12/31/2015
- Working with NEI/industry on the resolution to generic issues via the SFAQ process
- NRC to audit the corrective actions associated with the Milestone 1-7 cyber security inspection findings in CY2016 & CY2017

## **NRC Cyber Security Program**

Inspected 10 CFR 73.54 Basic Requirements:

1. Identify digital assets and communication systems associated with SSEP functions.
2. Apply & Maintain a Defense-in-Depth Protective Strategy. (portable media, scanning, data diode, etc).
3. Implement Security Controls to protect digital assets and communications systems.
4. Identify, Respond and Mitigate against cyber attacks.



## **NRC Cyber Security Program**

10 CFR 73.54 Basic Requirements:

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.

## Full Implementation (Milestone 8)

### Milestone 8 Activities:

- Full Implementation of controls on **all** CDAs
- Cyber Attack Mitigation and Incident Response
- Supply Chain
  - Adds security requirements relevant to vendors
- Enhance CDA integrity to prevent CDAs from accessing, receiving, transmitting, or producing unverified information
- Configuration Management
- Ongoing Evaluation and Management of Cyber Risk
- Effectiveness Reviews of the CSP program and controls

## **Cyber Security Plans Milestone 8 Preparations**

- Conducting tabletops, pilots, and workshops to develop additional guidance
- Regional inspectors included in Milestone 8 tabletop review to improve consistency, additional NRC cyber training has been developed
- NRC to initiate Milestone 8 inspections starting July 2017

## Cyber Reporting Requirement

- The Cyber Security Notification rulemaking became effective on December 2, 2015
- Implementation date – May 2, 2016
- RG 5.83 provides NRC guidance
- NEI guidance document (NEI 15-09)

## Cyber Security Event Notification Rule

- **One-hour notifications**
  - a cyber attack that adversely impacted SSEP function
- **Four-hour notifications**
  - cyber attack that could have caused an adverse impact to SSEP
  - suspected or actual cyber attack initiated by personnel with physical or electronic access to digital computer and communication systems
- **Eight-hour notifications**
  - After receipt or collection of information regarding observed behavior, activities, or statements that may indicate intelligence gathering or pre-operational planning related to a cyber attack
- **24-hour recordable events**

## Other Cyber Related Topics

- Staff evaluating cyber security for decommissioning units and ISFSIs
- New reactors (Part 52) cyber application
  - Same requirements as Part 50
  - Differences in CDA profiles, systems, and numbers
  - Different controls
- Updating applicable RGs associated with DBT, Security Training, and Insider Mitigation requirements consistent with Cyber Security Program



## Fuel Cycle Cyber Security

- NRC Commission approved high-priority rulemaking to develop cyber security requirements for fuel cycle facility licensees
- The rulemaking will be graded based on the consequence of concern for the facility type
- The proposed rulemaking should be sent to the Commission early in 2017
- The final rulemaking is targeted for 2018

## Full Cyber Implementation

- What does full cyber implementation mean?
- What does a running cyber program look like?
- The cyber security staff at the corporate and site level need awareness and understanding of NRC guidance and requirements.

**Cyber Security is a Program not a Project**

# Questions

