

An NRC Commissioner's Perspective on Cyber Security Regulation

Commissioner William C. Ostendorff
United States Nuclear Regulatory Commission

State Liaison Officers Conference
Rockville, MD
October 27, 2015

Key Principles

- NRC Oversight Role as Regulator
- Engagement with Stakeholders
 - Inter-Agency
 - Public
 - Industry
- Risk-Informed Approach

U.S. Inter-Agency Cooperation on Cyber Security



NRC Requirements

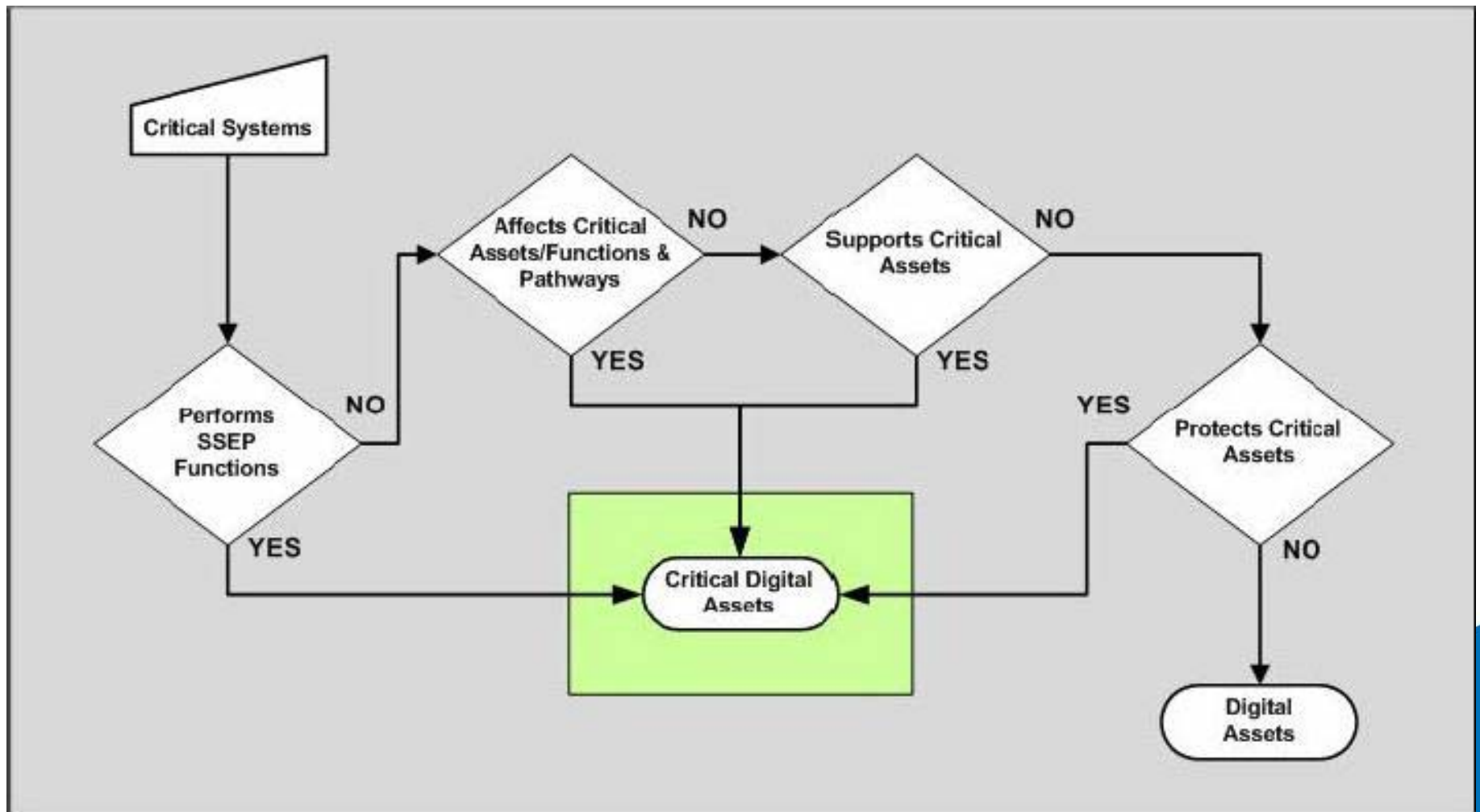
March 2009 Cyber Security Rule (10 CFR 73.54) –
Requires that nuclear power plant licensees:

- “Provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks”
- “Establish, implement, and maintain a cyber security program” to protect critical digital assets (CDAs).

Scope of 10 CFR 73.54

- **Safety-related and important-to-safety functions,**
- **Security functions,**
- **Emergency Preparedness functions, including offsite communications, and**
- **Support systems and equipment important to safety and security.**

Critical Digital Assets



Phased Implementation

Interim Milestones 1-7 (completed in 2012)

- Cyber Security Plans
- Addresses key threat vectors

Milestone 8 (site-specific implementation dates through 2017)

- Full cyber security program implementation
- Procedures and training

Milestones 1-7

- 1) Establish Cyber Security Assessment Team
- 2) Identify Critical Digital Assets
- 3) Incorporate Isolation features
- 4) Control portable and mobile devices
- 5) Enhance insider mitigation
- 6) Establish security controls for target set CDAs
- 7) Monitor and assess security controls

NRC Oversight

- Inspections of Milestones 1-7 planned for completion in 2015
- Inspections of Milestone 8 will begin in 2016



Consequence-Based Approach

- Graded approach
 - Focus NRC and licensee resources on most significant issues
 - Direct vs. Indirect CDAs

Consequence-Based Approach (continued)

- Grouping of CDAs
- Precludes need for each licensee to analyze common device types
- NRC developing templates and examples for efficiency and consistent implementation

Cyber Security at Fuel Cycle Facilities

- Currently, Fuel Cycle Facilities are under an Order addressing Additional Security Measures, including cyber security
- Gap analysis between orders and the need for rulemaking
- Commission directed rulemaking

What's Next?

- NRC continues to make significant progress
- Cyber Security will always be a challenge
- Stakeholder coordination essential
- Situational awareness