



NRC Cyber Security Regulatory Framework Update

Office of Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission

Overview



- Background
- Program Implementation
- Federal Energy Regulatory Commission (FERC) / North American Electric Reliability Corporation (NERC) Interactions
- International Activities
- Cyber Security Roadmap
- Ongoing and Future Activities
- Questions

2

Background



- Current Regulation: 10 CFR 73.54 "Protection of digital computer and communication systems and networks"
- Basic Requirements
 - Identify digital assets that must be protected
 - Safety, important-to-safety, security, and emergency preparedness functions
 - Defense-In-Depth protective strategy
 - Application of security controls to digital assets
 - Submission of a Cyber Security Plan and Implementation Schedule to NRC for review and approval
- Cyber Security Plan
 - Licensing document / required by regulation
 - Describes how cyber security program is established and maintained

3

Program Implementation



- Interim Milestones 1-7 (12/31/2012)
 - address key threat vectors for all Critical Digital Assets
 - Emphasis on target set equipment
- Milestone 8 (site specific date)
 - full cyber security program implementation
 - policies and procedures: training, attack mitigation, incident response, continuity of operations, etc.
 - completion of all design remediation actions, including those that require a refuel outage for implementation

4

FERC / NERC Interactions



- NRC Authority
- Energy Policy Act of 2005
- FERC Order 706/706B
 - recognizes potential for overlap
- NRC Public/Private Coordination
 - FERC Memorandum of Agreement
 - NERC Memorandum of Understanding
- SECY-10-0153
 - Implementation of the Commission's determination of systems and equipment within the scope of 10 CFR 73.54
- Recent Interactions
 - Coordination with FERC on their establishment of the Office of Energy Infrastructure Security

5

International Activities



- Supporting the International Atomic Energy Agency (IAEA) efforts in cyber security
 - Guidance on the application of cyber security controls to safety and digital instrumentation & control (DI&C) systems
 - Guidance on the development of a cyber Design Basis Threat model
 - Computer security assessment training and material development
 - Computer security incident response and forensics
- International Nuclear Security conferences
 - NRC hosted event in 2012
 - IAEA hosted event in 2013

6

Cyber Security Roadmap



- Provides an update to the Commission on the status of the implementation of cyber security requirements for power reactor licensees and Combined License applicants
- Outlines the approach for evaluating the need for cyber security requirements for the following four categories of the NRC licensees and facilities:
 - Fuel cycle facilities
 - Non-power reactors
 - Independent Spent Fuel Storage Installations
 - Byproduct materials licensees

7

Ongoing and Future Activities



- Update of regulatory framework
 - Will incorporate lessons learned from the oversight process
- NUREG development
- Cyber Security Roadmap Activities
- International and Intergovernmental Activities

8

Questions



9
