



Cyber Security Activities

NRC/FERC Joint Commission Meeting
June 7, 2018



James Andersen, Director Division of Physical & Cyber Security Policy, Office of Nuclear Security & Incident Response

- NRC Cyber Security History
- Full Implementation of Cyber Security Requirements
- Initial Results of Full Implementation Inspections
- NRC Cyber Security – What's Next

Cyber Security Programs Fully Implemented by Licensees in 2017

- 2002-2003: First cyber requirements
- 2009: Cyber security rule
- 2010: Interagency coordination
- 2012: Milestones 1-7, interim measures
- 2013: Graded-approach
- 2015: Cyber security notification rule
- 2017: Full implementation, Milestone 8

Full Implementation Requires that Licensees Address Multiple Controls

- Technical controls on all direct impact Critical Digital Asset (CDAs)
- Attack mitigation and incident response testing and drills
- Continuity of operations training & testing
- Configuration management

Additional Full Implementation Cyber Security Controls

- Supply chain
 - Adds security requirements relevant to vendors, contractors, and developers
- Ongoing evaluation and management of cyber risk
- Audit and accountability
 - Validates effectiveness of the cyber security program and controls

NRC Inspections Ongoing – Overall Positive Results

- Seven inspections are complete
- Number of inspection findings low
- Areas for improvement may need additional guidance:
 - Portable media & mobile device program
 - Critical digital asset assessments
- Plants under Construction

What's Next for the NRC in this Rapidly Changing Area

- The NRC staff will be conducting an overall cyber security assessment
- NRC staff will continue engagement with Federal Partners
- NRC staff will continue engagement with International Partners

Acronyms

- CDA – Critical Digital Asset
- CSP – Cyber Security Plan
- FERC – Federal Energy Regulatory Commission
- NEI – Nuclear Energy Institute
- NERC – North American Electric Reliability Corporation