RIC 2010

Part 73 and Cyber Security

Craig Erlanger
NSIR/DSP
March 9, 2010

Overview

- Background
- 10 CFR 73.54, Protection of Digital Computer and Communications Systems and Networks
- Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities
- Cyber Security Plans
- FERC / NERC Interactions
- Path Forward

Background

- Interim Compensatory Measures (2002)
  - Implementing guidance
- NUREG/CR-6847, Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants (2003)
- Design Basis Threat Order (2003)
- NEI 03-12, Security Plan, Training and Qualification Plan, and Safeguards Contingency Plan, Section 18 (2004)
- NEI 04-04, Cyber Security Program for Power Reactors (2005)
- 10 CFR 73.1, Design Basis Threat Rule (2007)
  - RG 5.69
- 10 CFR 73.54, Cyber Security Rule (2009)
  - DG-5022 / RG 5.71
  - NEI 08-09

10 CFR 73.54

- **High-level, Performance-Based, Programmatic**
  - **FOCUS: Prevention of Radiological Sabotage**
  - **Generic (i.e., not reactor-specific)**
  - **Consistent with regulatory approach for physical security**
- **Basic Requirements**
  - **Digital assets that must be protected**
  - **Defense-in-depth protective strategy**
  - **Application of security controls to digital assets**
  - **Implementation details maintained on site**
  - **Submission of Cyber Security Plans to NRC for approval**
- **Cyber Security Plans**
  - **Site-specific processes and criteria**

4

Regulatory Guide 5.71 - Overview

- **Regulatory Guide 5.71**
  - **Main Body**
  - **Appendix A (generic Cyber Security Plan template)**
  - **Appendix B (technical security controls)**
  - **Appendix C (operational/management security controls)**
- **Performance-Based, Programmatic**
  - **Consistent with NIST recommendations**
  - **Flexible and minimally prescriptive**
    - **– Burden on licensees to establish effective programs**
- **Alignment with Regulatory Guide 1.152, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants**

5

Cyber Security Plan

- **Licensing document / required by regulations**
  - **Will be incorporated into plant operating license**
- **Must describe how cyber security program is established and maintained**
  - **System level details not required or desired**
- **Essential elements – Plan must:**
  - **Describe the process for identifying CDAs**
  - **Describe the defensive model (protective strategy)**
  - **Reference a comprehensive set of security controls**
  - **Describe the process for addressing each control**
  - **Commit to maintaining adequate documentation**

6

Cyber Security Features included in System Designs

- Part 50
  - Establishes safety system design criteria to prevent and/or mitigate established, non-malicious design basis events
- Part 73
  - Requires security programs to prevent malicious acts from causing radiological sabotage
- Neither Part 50 or Part 73 requires inclusion of cyber security features as part of digital system designs
- If one or more design features are included voluntarily:
  - Will only be evaluated for impacts on system functionality and reliability during licensing reviews (safety systems only)
  - Efficacy of feature to perform security function(s) will be evaluated during NRC inspection of cyber security program

7

FERC / NERC Interactions

- Energy Policy Act of 2005
- FERC Order 706B
  - Recognizes potential for overlap
- Limits of NRC authority
  - Part 50 (non-malicious failure modes only)
  - Part 73 (safety, security, emergency prep only)
- NRC/NERC Memorandum of Understanding
  - Scope:
    - Information sharing
    - Exception request reviews
    - Inspections and enforcement

8

Path Forward

- Implement MOU with NERC
  - Plan to conduct several workshops
- Complete site-specific Cyber Security Plan reviews
  - New reactor COLAs
  - Operating reactors
- Develop Cyber Security Oversight Program (Inspection, Assessment, Enforcement)
  - Stakeholder input will be solicited

9

BACKUP SLIDES

10

Regulatory Guide 5.71 - Evolution

- **DG-5022 (2008)**
  - **Highly prescriptive**
- **RG 5.71 (Draft February 2009)**
  - **Based on NUREG/CR-6847 concepts**
  - **Intent to endorse NEI 08-09**
  - **Presented to ACRS**
- **RG 5.71 (Draft July 2009)**
  - **Incorporated ACRS comments**
  - **Based on NIST security controls**
  - **Included NRC-developed generic security plan template**
  - **Provided to COL applicants by letter**
- **RG 5.71 (Final Draft October 2009)**
  - **Provided to licensees & COL applicants by letter**

11