A Regulatory Approach to Cyber Security

Perry Pederson
Security Specialist (Cyber)
Office of Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission
Overview

Regulatory Framework
• Part 50 Safety and Part 73 Security
• Title 10 of the Code of Federal Regulations 73.54

Oversight Activities
• Regulatory Guide 5.71
• Regulatory Guide 1.152

Research Activities
• Cyber Security Roadmap
• Paradigm Shift

Questions

Agenda
Regulatory Framework

- Regulations
- Oversight and Inspection
- Regulatory Guidance
- Licensing
Cyber Security for Nuclear Reactors

**Regulatory Objective**
PREVENT RADIOLOGICAL SABOTAGE

**Requirements**
- 10 CFR 73.1 (Design Basis Threat)
- 10 CFR 73.54 (Cyber Security)

**Scope**
Systems that provide:
- Safety, Important-to-Safety functions
- Security functions
- Emergency Preparedness functions
- Support Systems whose failure would have an *Adverse Impact* on one of the above functions

**Guidance**
RG 5.71 & Appendices
Nuclear Energy Institute (NEI) 08-09 (Generic Cyber Security Plan Template)

**Implementation**
Oper. Rx Cyber Security Plan (10 CFR 50.34)
COLA Cyber Security Plan (10 CFR Part 52)

**NRC Licensing**
Safety Evaluation (Chapter 13)
Issue License Condition

**Approach**
Programmatic
Defense-in-Depth
Risk-informed

**Adverse Impact** = Compromise of support system impairs/defeats the functionality of a safety system, important-to-safety system, security system, or emergency response system

**Support Systems**
Support Systems whose failure would not have an *Adverse Impact* on a safety, important-to-safety, security, or emergency preparedness function fall under Federal Energy Regulatory Commission (FERC) regulations (i.e., North American Electric Reliability Corporation (NERC) cyber security standards)

**Memorandum of Agreement with FERC and Memorandum of Understanding with NERC**

**Approach**
Programmatic
Diversity and Defense-in-Depth
Deterministic

**Guidance**
RG 1.152 Rev 3
IEEE Std. 603, IEEE Std. 7-4.3.2
Design Acceptance Criteria (Part 52)

**Implementation**
Amendment Request (10 CFR 50.90)
Design Criteria Application (10 CFR 52)

**NRC Licensing**
Safety Evaluation (Chapter 7)
Issue License Condition

**Regulatory Objective**
SYSTEM FUNCTIONALITY & RELIABILITY

**Requirements**
- 10 CFR 50.34
- 10 CFR 50.55a
- 10 CFR 50 Appendix A (General Design Criteria)
- 10 CFR 50 Appendix B (Quality Assurance)
- 10 CFR 52.4

**Scope**
Systems that are:
- Safety-Related
- Important-to-Safety

**Approach**
System-level design features
Diversity and Defense-in-Depth
Deterministic

**Guidance**
RG 1.152 Rev 3
IEEE Std. 603, IEEE Std. 7-4.3.2
Design Acceptance Criteria (Part 52)

**Implementation**
Amendment Request (10 CFR 50.90)
Design Criteria Application (10 CFR 52)

**NRC Licensing**
Safety Evaluation (Chapter 7)
Issue License Condition
10 CFR 73.54

Title: Protection of digital computer and communication systems and networks

- Performance-Based, Programmatic (< 2 pages)
  - Provide high assurance against cyber attack
  - Integrated with Physical Security Program (10 CFR 73.55)

- Basic Requirements
  - Critical digital assets must be protected
  - Safety, important-to-safety, security, and emergency preparedness functions and support systems that can impact those functions
  - Defense-in-depth protective strategy
  - Records maintained for duration of license
Regulatory Guide 5.71

Title: Cyber security programs for nuclear facilities

- Form Cyber Security Team
- Identify Critical Digital Assets
- Apply Defensive Architecture
- Address Security Controls

1. Address each control for each critical digital asset, or
2. Apply alternative measures, or
3. Explain why a control is not applicable
Regulatory Guide 1.152

Title: Criteria for use of computers in safety systems of nuclear power plants

- A method for complying with the Commission’s regulations high functional reliability, design quality, and a secure development and operational environments

- The combination of this regulatory guide and the programmatic provisions under 10 CFR 73.54 and RG 5.71 address the secure design, development, and operation of digital safety systems
Oversight Activities

• Inspection Program
  – pilot process
  – inspector training
• Significance Determination Process
• Threat information sharing
  – Protected Web Server (PWS)
  – United States Computer Emergency Response Team (US-CERT)
  – Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
Research on Security of Digital Instrumentation and Control

- Security of Digital Platforms
- Network Security
- Security Assessments of Electromagnetic and Radio Frequency Vulnerabilities
- Quantification of Security Posture
- Reliability Impacts of Smart Grid
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.

• The paper 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
Paradigm Shift

Probable  Possible
Physical Security

Protecting People and the Environment
Questions