Nuclear Power Plants & Cyber Security

Scott A. Morris, Deputy Director
Reactor Security
Office of Nuclear Security and Incident Response

April 8, 2008

NRC Mission

- License and regulate the Nation's civilian use of byproduct, source and special nuclear materials to ensure adequate protection of public health and safety, promote the common defense and security, and protect the environment.

- Applicability to nuclear power plant instrumentation & control (I&C)
  - Any system that could impact safety, security and/or emergency preparedness/response

Nuclear Safety

- I&C Safety System Design Requirements
  - Well established and understood
  - Redundancy, Diversity, Independence
  - “Reasonable Assurance” standard

- Verification
  - Licensing Reviews
  - Inspections and Enforcement

Nuclear Security

- Design Basis Threat
  - Protect against “radiological sabotage”
  - Stand-alone or coordinated attacks
  - Performance-based approach
  - “High Assurance” standard

- Current security risk to safety systems is low because:
  - Existing design requirements
  - Older technology in use (analog or solid-state logic)

Post-9/11 Requirements

- Basis
  - Digital I&C retrofits increasing
  - New reactor designs
- Interim Compensatory Measures (2002)
- Design Basis Threat (2003, 2007)
  - Added cyber attack
- Proposed New 10 CFR 73.54 (2006)
  - Cyber security programmatic requirements
  - Alignment with FERC CIP Standards

Power Reactor Industry Actions

- Nuclear Energy Institute (NEI) 04-04
  - Risk-informed, performance-based program
  - Based on NRC requirements and guidance
  - Compatible with FERC CIP standards

- All power reactors committed to implement an NEI 04-04 program by May 2008

Potential Regulatory Issue

- NRC cyber-security requirements do not extend to power continuity systems
- NEI 04-04 implementation:
  - Is not compulsory
  - Scope includes systems outside NRC's regulatory purview
- FERC and NRC staff working to address this apparent regulatory issue