Power Reactor Cyber Security Program Assessment

Brad Bergemann
Cyber Security Branch
Division of Physical and Cyber Security Policy
Office of Nuclear Security and Incident Response

Agenda

- Opening Remarks & Introductions
- Objectives
- Assessment:
  - Background
  - Process
  - Feedback
  - Next Steps
- Questions & Comments

Objectives

- Identify key areas for improvement by capturing lessons learned from stakeholders.

- Use assessment feedback to further inform the outcome of Petition for Rulemaking (PRM)-73-18, “Petition to Amend 10 CFR 73.54, ‘Protection of digital computer and communication systems and networks.’”

Background

- March 2009, the Nuclear Regulatory Commission (NRC) published Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54

- December 2012, licensees completed Milestones 1-7

- June 2014, the Nuclear Energy Institute (NEI) submitted PRM-73-18

- September 2017, the NEI and licensees informed of the power reactor cyber security program assessment

- December 2017, licensees completed Milestone 8

- January 2019, the NRC initiated the assessment

Process

- Collected feedback from:
  - Nuclear power reactor licensees
  - Nuclear Energy Institute staff
  - Federal Energy Regulatory Commission staff
  - NRC Headquarters cyber security staff
  - NRC Regional cyber security inspection staff

- Conducted 2 public meetings (ML19024A051, ML19074A006) and 1 closed meeting (ML19163A386)

Feedback

- Main area identified for improvement is the scoping of critical digital assets (CDAs).
  - Current scoping criteria is on protecting CDAs from adverse impact.
  - Potentially, many CDAs currently being protected would not pose a risk to public health and safety.

- Factors that led to CDA scoping issues:
  - Rule and guidance interpretations
  - Milestone 1-7 inspections
  - Broad definitions and terms

- CDA numbers had a cascading effect on other programs.

Feedback Continued

- Other areas identified for improvement/consideration:
  - Adopting a more risk-informed graded approach
  - Providing additional criteria for alternate controls
  - Providing more credit for existing plant programs
  - Utilizing controls tailored to an industrial control system environment
  - Providing clarification for digital assets not categorized as CDAs
  - Updating the NRC policy to align with current North American Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards
  - Transforming the future cyber security inspection program

Feedback Continued

- Office of the Inspector General: Audit of NRC’s Cyber Security Inspections at Nuclear Power Plants (OIG-19-13)
  - Two recommendations:
    - Identify critical skill gap and closure strategies for future cyber security inspection staffing
    - Develop and implement cyber security performance measures which licensees can demonstrate sustained program effectiveness

Next Steps

- Finalize report and develop an action plan
- Goal: Initiate changes as appropriate to the power reactor cyber security program. Guidance documents to consider for revision include:
  - NEI 10-04, “Identifying Systems and Assets Subject to the Cyber Security Rule”
  - NEI 08-09, “Cyber Security Plan for Nuclear Power Reactors”
  - NEI 13-10, “Cyber Security Control Assessments”
  - Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities”
  - Develop new guidance that incorporates all previous guidance into one consolidated document.

Questions & Comments