U.S.NRC
Protecting People and the Environment

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

- Objectives
- Task Organization & Purpose
- Schedule
- Framework
- Questions & Comments

Objectives

- **In 2019, conduct an assessment of the power reactor cyber security program that captures the following:**
  - Effectiveness of the cyber security rule, guidance documents and licensees implementation;
  - Effectiveness of the full implementation inspection program and develop a path forward;
  - Lessons learned over the course of program implementation for the purposes of knowledge management and continuous improvement.
- **The assessment will result in a final report and support the staff assessment of PRM-73-18.**

Task Organization & Purpose

U.S.NRC
Protecting People and the Environment

- **The Assessment Team will consist of 3 personnel:**
  - 1 NRC staff from Cyber Security Branch;
  - 1 NRC staff from Nuclear Reactor Regulation;
  - 1 independent cyber security specialist from outside the NRC.
- **The Assessment Team will conduct multiple engagements with stakeholders to discuss, review and collect data to identify and determine the outcomes of the objectives.**

Schedule

- **Schedule of assessment activities:**
  - Kickoff public meeting: January 10, 2019
  - Engagement 1: week of January 28th
  - Engagement 2: week of February 11th
  - Engagement 3: week of February 25th
  - Engagement 4: week of March 11th
  - Mid-process public meeting: week of March 18th
  - Engagement 5: week of March 25th
  - Final public meeting: TBD (April or May)
  - Assessment final report: TBD (May or June)
  - Petition Review Board Closure Package to the Commission: NLT October 23, 2019
- **Specific dates and locations of engagements 1-4 to be determined.**

Framework

U.S.NRC
Protecting People and the Environment

- **Discussion and data collection framework:**

1. Discuss specific rule language and/or guidance documents that may have contributed to not correctly screening Digital Assets (DAs) as Critical Digital Assets (CDAs).
2. Discuss the processes used for assessing/screening the overall consequence to the Critical System (CS) and Safety, Security and Emergency Preparedness (SSEP) functions if a compromise of the CDA occurs.
3. Discuss the process used to identify CSs and CDAs including the criteria used to include or exclude each DA.
   a. How many DAs were screened as CDAs based on compromise NOT adversely impacting its function?
4. Discuss number of DAs identified based on 73.54(a)(1).
   a. Discuss number of DAs screened as CDAs (require protection) as a result of the analysis in 73.54(b)(1).
5. Discuss any differences (if applicable) between any DA/CDA assessments conducted pre-rule, for Milestone 2 (M2), and for full implementation and their impacts or insights.
6. Discuss and provide recommendations on approaches to further risk inform the CDA screening process.
7. Discuss formation of the Cyber Assessment Team and any changes over time (M2, full implementation, size, etc.) and their impacts (if applicable).
8. Discuss lessons learned from the full implementation inspections conducted to date and ideas for inspection efficiency.
9. Discuss self-assessment and licensee program/system testing and performance indicators as well as periodicity that could be used as input for cyber security oversight in the future.

Questions & Comments