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

- **Schedule**
- **Framework (Questions)**
  - **Status update**
  - **Opportunity for Additional Comments and Feedback**
- **Closing Comments**

Schedule

- ✓ Kickoff Public Meeting: 10 JAN 2019
- ✓ Stakeholder Engagements:
  - ✓ Duke: 13 FEB 2019
  - ✓ NextEra: 19 FEB 2019
  - ✓ Entergy: 26 FEB 2019
  - ✓ Exelon: 05 MAR 2019
  - ✓ NEI Workshop: 25 MAR 2019
  - ✓ FERC: 28 MAR 2019
- Status Public Meeting: 09 APR 2019
- Final Public Meeting: ~10 JUN 2019
- Final Report Complete: ~08 JUL 2019

Framework

1. Discuss the process used to identify Critical Systems (CS) and Critical Digital Assets (CDAs) including the criteria used to include or exclude Digital Assets (DAs).
2. Discuss the number of DAs identified based on 10 CFR 73.54(a)(1) and the number of DAs screened as CDAs as a result of the analysis in 10 CFR 73.54(b)(1).
3. Discuss specific rule language and/or guidance documents that may have contributed to screening DAs as CDAs which are not needed to protect against cyber attacks, up to and including the DBT, as described in 10 CFR 73.1. Provide examples of each of the following types of CDAs that fit this description, if possible: Safety; Security; Emergency Preparedness; Support Systems and Equipment, if compromised, that would adversely impact SSEP functions; and BOP.
4. Discuss what changes occurred as a result of the Milestone 1-7 inspections in relation to CDA identification.
5. Discuss technical controls that are overly conservative that have no direct relationship to the objective of the cyber rule (10 CFR 73.54(a)). Provide specific examples.
6. Discuss defense in depth. Are there regulatory requirements or guidance that lead to over-conservative licensee actions?
7. Discuss the use alternate controls. Is there language in the Cyber Security Plans (CSPs) or guidance documents that makes the process burdensome and difficult to use? Are there additional areas licensees could use to justify the use of alternate controls, but are not allowed to use?
8. Discuss formation of the Cyber Assessment Team (CSAT) and any changes over time, and their impacts. What is the role of the CSAT after full program implementation? Have you incorporated the CSAT into other processes? How many hours are spent on CSAT functions?
9. What is the cost of maintaining the Cyber Security Program (e.g., full-time equivalents)?

Framework Continued

U.S.NRC
Protecting People and the Environment

10. Have you decided to not implement a digital upgrade due to cyber security requirements and what actions are you planning instead?
11. Discuss lessons learned from the full implementation inspections conducted to date and ideas for inspection efficiency.
12. Discuss possible ways the inspection process can be transformed after the NRC completes the first round of inspections in 2020.
13. Discuss programs used to ensure the ongoing health of the Cyber Security Program that can be used by the NRC to assess the compliance to the Facility Operating License Condition for the CSP.
14. Discuss methods used to ensure the ongoing health of the Attack Mitigation and Incident Response capability (reference CSP E.7) including Cyber Security Incident Response Team response and drills.
15. Discuss initial design and testing of the boundary devices and network monitoring systems that has been performed to demonstrate the capabilities of these barriers to site CDAs. Discuss any ongoing testing of these systems to monitor the ongoing health of these capabilities.
16. Discuss any unexpected impacts to Plant Operations, Security, or EP based on the application of Cyber Security Controls. Examples are plant power reductions, equipment/process reliability issues, etc.
17. Time permitting, discuss the Cyber Security Event Notification rule and guidance for potential changes/revisions [end].

Closing Comments

U.S.NRC
Protecting People and the Environment