Cyber Security Programs: Safe, Secure, Risk-Informed While Minimizing Licensee Burden

Russell Felts, Deputy Director
Cyber Security Directorate, Office of Nuclear Security and Incident Response

Cyber Rule Issuance

- Current Regulation: 10 CFR 73.54 "Protection of digital computer and communication systems and networks"
- Basic Requirements
  - Safety, important-to-safety, security, and emergency preparedness functions
  - Submission of a Cyber Security Plan and Implementation Schedule to NRC for review and approval
  - Identify digital assets that must be protected
  - Defense-In-Depth protective strategy
  - Application of security controls to digital assets
  - Detect, respond to, and mitigate adverse effects of cyber attacks
- Cyber Security Plan
  - Licensing document / required by regulation
  - Describes how cyber security program is established and maintained

NRC and FERC

- Avoiding dual regulations
  - NRC, FERC, and NERC discussed balance-of-plant
  - Industry response to bright-line survey
  - Commission policy direction
  - Cyber Security Plans revised to incorporate BOP within scope
  - NRC and FERC collaborated to right-size BOP cyber
  - Agreement captured in NEI 13-10

NEI 13-10

NRC's perspective on NEI 13-10

- Increase focus on most consequential assets
- NRC proposed a consequence-based graded approach to address cyber security controls
- NEI 13-10 assessment templates help licensees focus resources appropriately, and minimize the burden of program implementation

NEI 13-10 Revisions 0, 1, and 2

NEI 13-10, Revision 0

- Defines direct and indirect CDAs
- Provides the method for determining whether a CDA is direct or indirect
- Defines the minimum set of security measures that address the required technical security controls for the indirect CDAs

NEI 13-10, Revision 1

- Incorporates a template and examples for performing the NEI 13-10 analysis to determine whether a CDA is direct or indirect and assess application of controls

NEI 13-10, Revision 2

- Incorporates a streamlining method for performing direct CDA assessments of technical security controls by grouping CDAs based on CDA technical capabilities
- Incorporates CDA class criteria for the simplest direct CDAs (A.1 Class)
- Incorporates a template for A.1 CDA technical security control assessments

NEI 13-10 Revision 3 and 4

NEI 13-10, Revision 3

- Incorporates guidance to identify low consequence balance of plant (BOP) CDAs:
  - BOP CDAs that are not relied upon to mitigate accidents or transients (i.e., equipment and systems that are not used to support the emergency operating procedures)
  - the BOP CDA's failure or cyber compromise does not prevent safety-related structures, systems, and components from fulfilling their safety-related functions
- Incorporates the minimum set of security measures that address required technical security controls for these BOP CDAs

NEI 13-10, Revision 4

- Incorporates criteria for five additional CDA classes (A.2, A.3, B.1, B.2, B.3) and associated templates for technical security control assessments


U.S.NRC
Protecting People and the Environment
RIC 2016
Questions?