Risk-Informing Physical and Cyber Security Programs

JULY 23, 2019

Review of Principles

- Where used in 10 CFR 73.55 and related guidance, the concept of “high assurance” of adequate protection is equivalent to “reasonable assurance”
- All outcomes of the process must ensure that reasonable assurance of adequate protection is maintained
  - Conclusion should be made considering overall capabilities of the physical protection program, rather than an individual program component
- Regulatory standards already include appropriate margin that the Commission deemed necessary to provide for adequate protection; there is no requirement for additional margin beyond these regulatory standards

Review of Principles

- Risk-informing criteria and processes should reflect realism
- Performance-based approaches and data are preferred
- Approaches will likely use qualitative and semi-quantitative analyses as quantitative data may not be available or feasible to produce
- Decisions may consider insights from safety and engineering assessments, and capabilities described in the facility licensing basis

Physical Security – Tier 1 (July 19, 2019)

- Tier 1 Projects
  - Revision to Section 21 of NEI 03-12, *Security Plan Template*
    - NRC endorsed risk-based methodology to identify implementation of Compensatory Measures
    - Implementation Workshop (June 25-27)
    - Next Steps
  - Revision to NEI 09-05, Guidance on Unattended Openings
    - Closed meeting on July 23
    - Employing realism and consideration of three-dimensional unattended opening testing conducted by Sandia National Labs

Physical Security – Tier 1 (July 19, 2019)

- Tier 1 (continued)
  - Regulatory Guide 5.81, *Target Set Identification and Development*
    - Comments distributed to NRC on July 1
  - Criterion 3 of RG 5.81 and Adversary Timelines
    - Industry team in process of review of NUREG-7145, *Security Assessment Guide*
    - Specific focus pertaining interdiction, delay, and neutralization

Physical Security – Tier 2 (July 19, 2019)

- Tier 2
  - Gain efficiencies through flexible post staffing and rotation requirements
  - Gain efficiencies by basing security equipment surveillance/testing activities on performance and reliability data (i.e., not prescriptive requirements)
  - Review of previous “Delivering the Nuclear Promise” initiatives

- Team Meeting on July 24

Cyber Security – Tier 1 and 2 (July 19, 2019)

- Tier 1
  - Qualitative risk-informing considerations in cyber security:
    - Transforming the NRC cyber security inspection process
    - Right-sizing cyber security scoping of CDAs and cyber security controls
    - Revision to cyber security guidance, as appropriate
- Tier 2
  - Changes to the cyber security rule, consistent with NEI's petition for rulemaking

Questions?