Risk-Informing Physical and Cyber Security Programs

MARCH 21, 2019

What is Risk-Informing Security?

- The holistic process of considering the likelihood of attack, likelihood of adversary success, and resulting level of threat consequences in the design, operation and management of a security program
  - Outcomes of this process may inform potential changes to security plans, organizations, systems, and implementing measures

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

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

Planned NEI Initiatives – Physical Security

- Revise criterion #3 in Regulatory Guide (RG) 5.81 to permit consideration of the capabilities of a site protective strategy (e.g., likelihood of neutralizations)
- In RG 5.81, define/characterize “desirable” and the relationship of this term to level of protection
- 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)
- Update guidance to provide realistic assessments of 3-D pathways

Planned NEI Initiatives – Physical Security

- Longer-term action
  - Consider a consequence-based security performance standard for existing fleet using insights from the physical security for advanced reactors rulemaking (SRM-SECY-18-0076)
    - This includes consideration of containment features

Planned NEI Initiatives – Cyber Security

- 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
- Longer-term action
  - Changes to the cyber security rule, consistent with NEI's petition for rulemaking

Questions?