Risk-Informing Security

March 21, 2019

Key Messages

- The staff has made substantial progress in the use of risk insights in the NRC's security oversight program.

- The staff continues to advance the application of the Commission's direction regarding the concept of reasonable assurance in the security construct.

- The staff is seeking input from the industry and other stakeholders to help shape ongoing and future efforts to risk-inform security.

Concept of Risk-Informing Security

- What It Is
  - Focus on Realism
    - Further incorporate the concept of reasonable assurance
  - Reliance on Qualitative or Semi-Quantitative Analyses for Physical Security
    - Quantitative data may not be readily available or feasible to produce for physical security events
    - Cyber security is better positioned to leverage quantitative analyses

Concept of Risk-Informing Security

- What It Isn't
  - Dependence on "PRA-like" Analyses for Physical Security
    - Most physical and cyber security events are not random events, hence quantifying risk poses a challenge.
    - However, conditional risk can be estimated using PRA-like analyses.
  - Mechanism to Change the DBT
    - The DBT must be included in any risk-informing activity
    - A process exists to evaluate the DBT

Working Definition

- The use of risk information, including threat information, the likelihood of adversary success, and resulting level of consequences of the threats posed by the design basis threat, in the evaluation of a security program and its implementing measures.

Current Activities

- Force on Force (FoF) Realism
  - Threat assessment information is being included in exercise scenario development
- Binning of FoF Tactics
  - The results of intelligence analysis of the tactics used by the mock adversary force are categorized and used to evaluate scenarios
- Risk-Informed Compensatory Measures
  - A risk-informed process to determine the implementing timelines for security compensatory measures
    - Based on site-specific threat conditions

Current Activities (Cont'd)

- Baseline Security Program Revision (including Inspection Procedures)
  - Use of risk-informed insights to determine the appropriate level of oversight
    - High assurance of adequate protection is equivalent to reasonable assurance
- Decommissioning Rule
  - Use of risk insights to determine the appropriate security regulations needed during decommissioning process
    - Current regulations require continued adherence to all program requirements

Current Activities (Cont'd)

- Cyber Security Control Assessments Guidance (NEI 13-10)
  - NRC reviewed and provided input to this industry guidance document that streamlines the process for addressing the application of cyber security controls to a large number of CDAs.
- Licensing Actions (50.54(p) reviews)
  - Use of risk insights to determine appropriate depth of review to ensure adequate protection
- Office-level Guidance to Staff
  - NRC program offices have issued guidance to the staff on applying the concept of reasonable assurance (ML18240A410 & ML19015A290)

Areas of Further Interest

- Consequence-based Security for Advanced Reactors
- Vulnerability Assessments, to include modeling and simulation
- Use of Safety Information in Security Activities
- 2019 Power Reactor Cyber Security Assessment
- Potential Focused Research
- Regulatory Hurdles to Innovation/New Technologies

Big Picture for the Future of Risk-Informed Security Activities

- Scope
  - Which facilities will be included in this effort?
- Vision
  - Why are we focusing on this? What type of results do we foresee?
- Culture
  - How do we embrace risk insights? How do we shift mindsets away from solely quantitative (e.g., PRA) constructs?
- Indicators
  - What does success look like moving forward?