U.S.NRC

United States Nuclear Regulatory Commission

*Protecting People and the Environment*

# Discussion of Draft Proposed Rule Text for Fuel Cycle Cyber Security

**Public Meeting**

**Thursday May 19, 2016**

# Category 3 Meeting

Public participation is actively sought at today's meeting. The purpose of this meeting is to hold discussions with stakeholders regarding the cyber security proposed rulemaking for fuel cycle facilities.

The handout provides the draft proposed rule text and should be considered a work in progress.

# Agenda

- Introductions, status update, and timeline

- Discuss draft proposed rule text

- Discuss topics for the July 2016 public meeting

# Status Update and Timeline

- Regulatory basis completed in March 2016 (81 FR 21449)
- Two additional public meetings July 2016 (guidance), and August 2016 (guidance)
- Proposed rule due to the Commission by March 17, 2017

# Structure of Draft Proposed Rule Text

a) Applicability

b) Cyber security program performance objectives

c) Consequences of concern

d) Cyber security program

e) Cyber security plan

f) Configuration management

g) Biennial review of the cyber security program

h) Event reporting and tracking

i) Records

# (a) Applicability

- Fuel cycle facilities – conversion, deconversion, enrichment, fuel fabrication, and reprocessing
- Date to submit cyber security plan as a license amendment request (e.g., 5 months after final rule)
- NRC reviews and approves cyber security plan (5 months is standard review time)
- Implementation of cyber security plan – phased approach under consideration:
  - Vital digital assets identified (e.g., 4 months after NRC approves cyber security plan)
  - Full implementation (e.g., 12 months after NRC approves cyber security plan)

# (b) Cyber security program performance objectives

- Protect vital digital assets
- Detect cyber attacks associated with a consequence of concern
- Respond to cyber attacks associated with a consequence of concern
- Recover from cyber attacks associated with a consequence of concern

# (c) Consequences of concern

- Four types of consequences of concern
  - Active - safety (applies to all facilities)
  - Latent - safety and security (applies to all facilities)
  - Latent - safeguards (applies to Category II facilities)
  - Latent - design basis threat (applies to Category I facilities)
- Intent is to prevent a cyber attack that:
  - directly results in a safety consequence of concern (active); or
  - compromises a function needed to prevent, mitigate, or respond to a safety/security/safeguards/design basis threat event associated with a consequence of concern (latent)
- Consequence thresholds informed by existing regulatory requirements

# (d) Cyber security program

- Revised approach from a risk management framework to a consequence-based cyber security program
- (1) Establish a Cyber Security Team
  - Management structure instead of authorizing official
  - Adequately staffed, trained, qualified, and equipped
- (2) Establish and maintain a set of cyber security controls for each applicable type of consequence of concern
  - Intent is for each facility to provide a set of controls for “Active - safety” and “Latent - safety and security”
  - Other consequences of concern applicable only at certain facilities (i.e., “Latent - safeguards” at Category II and “Latent - design basis threat” at Category I)
  - Address each control family (examples in draft regulatory guide)

# (d) Cyber security program (continued)

- (3) Identify digital assets and support systems that could result in a consequence of concern, if compromised
  - Intent is to document these digital assets
  - Digital assets that are part of a classified system are excluded
- (4) Determine vital digital assets
  - Identified in (d)(3) but have no alternate means
  - Alternate means must be protected from a cyber attack (examples will be in the draft regulatory guide)

# (d) Cyber security program (continued)

- (5) Validation testing for vital digital assets
  - Confirms network location
  - Provides an established boundary for implementing controls
- (6) Implementing procedures for cyber security controls
  - Apply applicable controls to vital digital assets (i.e., those with no alternate means)
  - Control parameters can be tailored to digital assets
  - Compensatory measures instead of plans of actions and milestones

# (e) Cyber security plan

- Must be submitted for NRC review in accordance with paragraph (a)
- (1) Considers site specific conditions
- (2) Documents the applicable sets of cyber security controls
- (3) Includes measures for incident response and recovery (examples will be in the draft regulatory guide)
- (4) Supporting documentation maintained onsite

# (f) Configuration management

- Evaluate facility modifications to ensure performance objectives are met prior to operating associated digital assets

- A facility modification may:
  - Add a previously unconsidered digital asset
  - Remove an alternate means for a digital asset that may create a vital digital asset requiring cyber security controls

# (g) Biennial review of the cyber security program

- Minimum 24 month review instead of an annual review and 3-year reaccreditation

- No independent assessment required

- Licensee documents, tracks, and addresses internal findings, deficiencies, and recommendations that result from:
  - (1) Analysis of program effectiveness and adequateness;
  - (2) Review of implementing procedures; and
  - (3) Vulnerability evaluation

# (h) Event reporting and tracking

- Follow existing regulatory requirements for notifications to the NRC

- When known, inform the NRC that the notification is a result of a cyber attack

- 24 hour reportable for:
  - (1) Failure, compromise, degradation, or vulnerability in a required cyber security control
  - (2) Compromise of vital digital asset for nuclear material control and accounting at Category I or II facilities – no associated regulatory requirement exists

# (i) Records

- Retain supporting documentation as a record

- Maintain records for inspection

- Maintain superseded records for 3 years

# Next Public Meetings

- July and August 2016 meetings
- Both in Rockville, MD -- bridge lines will be provided
- Suggested topics:
  - NRC staff presents draft regulatory guide (July)
  - Stakeholders provide initial feedback (July)
  - Seek additional stakeholder feedback on draft regulatory guide (August)
- Any additional topics?