U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Discussion on the Updated Draft Proposed Rule Text and the Related Draft Regulatory Guide for Cyber Security at Fuel Cycle Facilities

Public Meeting

Thursday August 25, 2016

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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 and related guidance for fuel cycle facilities.

The handout provides the draft proposed rule text and related draft guidance.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

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Agenda

- Introductions, status update, and project timeline
- Overview of the updated draft proposed rule text
- Discuss the draft regulatory guide
  - Overall staff guidance
  - Cyber security plan template
  - Controls to protect vital digital assets (VDAs)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Status Update and Timeline

- Advisory Committee on Reactor Safeguards (ACRS) briefings — November & December 2016
- Proposed rule to the Commission — March 2017
  - SECY Paper with:
    - *Federal Register* notice (proposed rule language and statements of consideration)
    - Environmental assessment
    - Regulatory analysis
    - Backfit analysis
  - Draft regulatory guide is separate package but in parallel review
- Concurrent formal comment period expected for proposed rulemaking and draft regulatory guide (estimate) — June – August 2017

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Updated Draft Proposed Rule Text

- Additions:
  - Date for current applicants to submit cyber security plan
- Deletions:
  - Recovery no longer a cyber security program performance objective
  - Cyber security control families no longer listed
  - Support systems no longer need to be identified and addressed unless associated with a vital digital asset
- Changes:
  - Reordered the consequences of concern (highest to lowest) based on the comprehensiveness of the associated cyber security controls
  - Added language clarifying that countermeasures to a cyber attack are taken to address cyber security controls
  - Edits to the rule language for clarity and alignment with draft regulatory guide

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Draft Regulatory Guide

- It is an early draft – feedback is appreciated
  - Suggest examples, identify text that needs clarification, and note any errors or oversights
  - Separate formal comment period with anticipated meetings
- Provides one method of satisfying the proposed regulation
- Includes text in main body that discusses the features of the rule, as well as appendices for use or reference:
  - Appendix A provides a cyber security plan template
  - Appendix B contains cyber security controls for VDAs associated with any consequence of concern
  - Appendices C – F contain cyber security controls for VDAs associated with specific consequences of concern

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Draft Regulatory Guide Chapters

A. Introduction

B. Discussion

C. Staff Regulatory Guidance

D. Implementation

Supporting glossary, references, and appendices

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

A. Introduction

- Purpose & applicability
- Applicable regulations
  - 10 CFR 73.53
  - Conforming changes to 10 CFR Part 40 (§§ 40.31 and 40.32) and Part 70 (§§ 70.22 and 70.32)
- Related guidance
- Purpose of regulatory guides

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

B. Discussion

- Reason for development
- Background
  - Overview of each section in draft regulatory guide
  - Table B-1 has timeline for phased implementation
- Harmonization with international standards
- Documents discussed in staff regulatory guidance

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

C. Staff Regulatory Guidance

1. General Requirements
2. Cyber Security Program Performance Objectives
3. Cyber Security Team
4. Cyber Security Plan
5. Consequences of Concern
6. Identification of Digital Assets ~~and Support Systems~~
7. Cyber Security Controls
8. Implementing Procedures and Interim Compensatory Measures
9. Configuration Management
10. Biennial Review
11. Event Reporting and Tracking
12. Recordkeeping

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

C.1 General Requirements

Provides an overview of each rule concept

1. Cyber Security Team
2. Cyber security plan
3. Identifying digital assets
4. Applying cyber security controls
5. Implementing procedures and interim compensatory measures
6. Managing the cyber security program

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

C.2 Cyber Security Program Performance Objectives

10 CFR 73.53(b)

- Detect a cyber attack capable of causing a consequence of concern
- Protect against a cyber attack capable of causing a consequence of concern
- Respond to a cyber attack capable of causing a consequence of concern

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

C.3 Cyber Security Team

10 CFR 73.53(d)(1)

- Responsibilities of the team
- Makeup of the team, training, and qualifications
- Management structure and relationship to operations

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

C.4 Cyber Security Plan

10 CFR 73.53(e)

- Reviewed and approved as NRC license amendment request
- Template for the plan is provided in Appendix A
- Documents program requirements for establishing and maintaining:
  - Cyber Security Team; and
  - Cyber security controls specific to each of the applicable types of consequences of concern
- Describes measures for:
  - Management and performance of the cyber security program; and
  - Incident response to a cyber attack affecting VDAs

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

C.5 Consequences of Concern

10 CFR 73.53(c)

- Details are provided for each consequence of concern
- Shows relationship of facility types to the consequences of concern
- How should a VDA be addressed that has more than one consequence of concern associated with it?
- Consequences of concern are ordered (highest to lowest) based on the comprehensiveness of the associated cyber security controls

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

C.6 Identification of Digital Assets ~~and Support Systems~~

10 CFR 73.53(d)(3)

- Provides a methodology for identifying digital assets and determining VDAs
- Discusses the characteristics of an acceptable alternate means that can be identified for digital assets
- Describes VDAs and associated boundaries, support systems, and potential grouping

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

C.7 Cyber Security Controls

10 CFR 73.53(d)(2) and (d)(5)

- A cyber security control is a performance specification established to provide an element of protection against specific cyber attack vectors
- A cyber security control is addressed by applying countermeasures to the cyber attack vector(s)
- Different cyber security controls are addressed by applying various countermeasures that are needed in combination to adequately protect against the cyber attack vector(s)
- A specific cyber security control should not be considered adequately addressed by the countermeasures taken to address another cyber security control (i.e., one control should not credit another)
- If a VDA is associated with more than one consequence of concern, it is expected that the licensee would apply the most comprehensive cyber security controls

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

C.8 Implementing Procedures and Interim Compensatory Measures

10 CFR 73.53(d)(5)(ii) and (d)(6)

- Implementing procedures are required to document the countermeasures to a cyber attack taken to address a cyber security control for a given VDA

- Interim compensatory measures are required when countermeasures are degraded
  - Demonstrate the cyber security program performance objectives are met
  - Interim compensatory measures are temporary, until a permanent countermeasure can be approved for use

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

C.9 Configuration Management

10 CFR 73.53(f)

- Additions or changes to the facility, or activity associated with a consequence of concern or a VDA,are reviewed for cyber security impact
  - Modifications to existing VDAs or procedures may be required prior to making the planned change

- Cyber security considerations should be integrated into the facility design and maintenance process
  - This is an ongoing effort

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

C.10 Biennial Review

10 CFR 73.53(g)

- Complete a comprehensive review of the cyber security program every 24 months
  - The process should be developed into procedures

- The results of the review could involve changes to the program or any VDAs, as well as a review of supporting documentation and analyses

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

C.11 Event Reporting and Tracking

10 CFR 73.53(h)

- Follow normal NRC event reporting along with:
  - Notifying the NRC if an event is the result of a cyber attack
  - Updating an existing event report upon discovery that the event involved a cyber attack

- A licensee must record the following events within 24 hours of discovery and track them to resolution:
  - Failure, compromise, degradation, or vulnerability in an applied cyber security control
  - Compromise of vital digital asset for nuclear material control and accounting at Category I or II facilities

- Voluntary notifications regarding cyber are encouraged

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

C.12 Recordkeeping

10 CFR 73.53(i)

- Retain supporting documentation as a record
  - Examples of records are provided
- Maintain records for NRC inspection
- Maintain superseded records for 3 years

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Appendix A: Cyber Security Plan

- A cyber security plan is required to be submitted for NRC review
- The template provides specific licensee actions and requirements regarding cyber security
- Cyber security plan must consider site specific conditions
- The applicable cyber security controls must be included in the plan submission and should follow the format of Appendices B – F
- Should the licensee choose to not utilize the NRC template for their cyber security plan, the licensee must demonstrate the requirements in 10 CFR 73.53(e) are addressed

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Appendix B: Controls for VDAs associated with all consequences of concern

- Contains cyber security controls that NRC considers applicable for VDAs associated with all consequences of concern
- The licensee can choose to adopt this appendix directly and attach it to their cyber security plan
- Should the licensee choose to develop its own controls, it must demonstrate that the controls provide the capability to prevent a cyber attack from causing a consequence of concern

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Appendix C – F: Additional controls for VDAs based on consequence of concern

- Contains additional controls that, in combination with the controls from Appendix B, NRC considers adequate to effectively address cyber security for VDAs associated with a particular consequence of concern
- The licensee can choose to adopt these appendices (as applicable) and attach them to their cyber security plan
- Should the licensee choose to develop their own controls, it must demonstrate that the controls provide the capability to detect, protect against, and respond to a cyber attack capable of causing a consequence of concern

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Next Meetings

- ACRS Subcommittee Digital Instrumentation & Control briefing in November 2016
  - NRC staff anticipates the public will be invited but this is formally at the discretion of ACRS
- ACRS Full Committee briefing in December 2016
  - NRC staff anticipates the public will be invited but this is formally at the discretion of ACRS
- Public meetings to solicit feedback on the proposed rule and the draft regulatory guide during the formal comment period(s)
  - Consistent with cumulative effects of regulation initiative