Handout on Potential Considerations for the Fuel Cycle Cyber Security Proposed Rulemaking

Public Meeting on February 18, 2016

The following potential considerations for development of draft proposed rule language are being made available to support the public meeting on February 18, 2016, from 1:00pm-3:00pm. This handout is intended to facilitate discussions, enhance stakeholders' understanding of the NRC staff's proposals, and support stakeholders ability to provide feedback.

The potential considerations for development of draft proposed rule language identified for discussion in this document are not intended to specifically or comprehensively represent the NRC's final regulatory position. Publication and solicitation for feedback during the public meeting is intended to support the NRC staff's development of draft proposed rule language. Once completed, the proposed rule language will be published in the *Federal Register* for formal comment. Comments received on the potential considerations below will be considered by the NRC staff, but are not part of the formal comment period. The approach discussed below is subject to change based upon refinement of the policy issues, future public meetings, and internal staff reviews.

Potential considerations for development of draft proposed rule language include the following:

1. Applicability
    a. Each applicant or licensee subject to the requirements of 10 CFR 70.60.
    b. Each applicant or licensee of a uranium hexafluoride conversion or deconversion facility licensed under 10 CFR Part 40.
    c. By [date], each licensee shall submit a cyber security plan as specified in 10 CFR 40.22(XXX) or 10 CFR 70.22(XXX), as applicable.

2. Cyber security program objectives
    a. Utilize a risk management framework.
    b. Identify assets associated with a consequence of concern.
    c. Protect assets associated with a consequence of concern by selecting, applying, and maintaining appropriate cyber security controls.
    d. Provide cyber security training appropriate for facility personnel.
    e. Ensure facility personnel are qualified to perform their assigned duties and responsibilities.
    f. Apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from a cyber attacks.
    g. Maintain configuration management of assets associated with a consequence of concern.

3. Consequences of concern
    a. Active (cyber attack directly causing a safety consequence of concern):
        i. A radiological exposure of 25 rem or greater for any individual;
        ii. Soluable uranium intake of 30 mg or greater for any individual outside the controlled area; or
        iii. An acute chemical exposure that could lead to irreversible or other serious, long lasting health effects for any individual.

b. Latent (cyber attack that causes the compromise of a function needed to prevent, mitigate, or respond to an event associated with safety, security, safeguards consequence of concern):
    i. A radiological exposure of 25 rem or greater for any individual;
    ii. Soluable uranium intake of 30 mg or greater for any individual outside the controlled area;
    iii. An acute chemical exposure that could lead to irreversible or other serious, long lasting health effects for any individual;
    iv. Unauthorized removal of special nuclear material of moderate strategic significance as specified in 10 CFR 73.67(d);
    v. Loss of control and accounting of special nuclear material of moderate strategic significance as specified in 10 CFR 74.41(a)(1)-(4); or
    vi. Loss or unauthorized disclosure of classified information.
c. Latent (cyber attack that causes the compromise of a function needed to meet the performance objectives for the design basis threat):
    i. 10 CFR 73.1(a)(1);
    ii. 10 CFR 73.1(a)(2); or
    iii. 10 CFR 74.51(a)(2)-(5), as applicable.

4. Risk management framework
    a. Establish and maintain a Cyber Security Team responsible for the cyber security program.
    b. Identify assets that, if compromised by a cyber attack, would directly cause an active consequence of concern. EXCEPTION – classified assets approved or accredited by another Federal agency.
    c. Identify assets that provide functions needed to prevent, mitigate, or respond to a latent consequence of concern. EXCEPTION – classified assets approved or accredited by another Federal agency.
    d. Conduct validation testing for assets identified.
    e. Establish a baseline set of cyber security controls.
    f. Select and apply tailored cyber security controls from the baseline set to identified assets. EXCEPTION – if an equivalent function provided by an alternate means maintains the capability to prevent, mitigate, or respond to a latent safety, security, or safeguards consequence of concern.
    g. Provide control implementation plans for identified assets.
        i. Addresses the applicable cyber security controls.
        ii. Maintains plans of action and milestones for cyber security controls that are not fully implemented.
            1. Plans of action and milestones are documented, tracked to completion, and available for inspection by NRC staff.
            2. The licensee's Authorizing Official reviews and approves the plans of action and milestones quarterly.
    h. Engage an independent assessment that is documented in a security assessment report.
        i. The control implementation plans are established, implemented, and maintained correctly;
        ii. The cyber security controls are operating as intended; and
        iii. The cyber security program objectives are met.

i. Designate a senior licensee official as the Authorizing Official.
    i. Reviews the security assessment report, control implementation plans, and plans of action and milestones; and
    ii. Determines that assets are authorized to operate given the level of risk.

5. Cyber security plan
    a. Ensures the cyber security program objectives are met.
    b. Describes how the regulatory requirements will be implemented and maintained.
    c. Is implemented through written policies and procedures.
        i. Not submitted for Commission review and approval.
        ii. Subject to inspection by the NRC staff.
    d. Accounts for site-specific conditions that affect implementation.
    e. Describes the baseline set of cyber security controls.
    f. Includes measures for incident response and recovery from a cyber attack affecting identified assets.
        i. Maintain the capability for timely detection and response;
        ii. Mitigate the impacts of a consequence of concern;
        iii. Identify and correct exploited vulnerabilities; and
        iv. Restore affected systems, networks, and equipment.

6. Periodic review of the cyber security program
    a. Performed at least every twelve (12) months (or as necessary based on site-specific analyses, evaluations of cyber security vulnerabilities, or performance indicators).
    b. Analyzes the effectiveness and efficiency of the program.
    c. Reviews control implementation plans.
    d. Includes a vulnerability evaluation of the cyber security controls and defensive architecture protecting identified assets.
    e. Documents, tracks, and addresses findings, deficiencies, and recommendations resulting from these analyses, evaluations, and performance indicators.

7. Reauthorization to operate
    a. Performed at least every thirty-six (36) months (or as necessary based on site-specific analyses, evaluations of cyber security vulnerabilities, or performance indicators).
    b. Evaluation of control implementation plans (includes plans of action and milestones) for identified assets.
    c. Engage an independent assessment that is documented in a revised security assessment report.
    d. Authorizing Official
        i. Reviews the revised security assessment report, control implementation plans, and plans of action and milestones; and
        ii. Determines that assets are authorized to operate given the level of risk.

8. Event reporting
    a. Make notifications as required under existing regulations.
    b. Inform the NRC, when known, that the notification is a result of a cyber security event.

i. Within twenty-four (24) hours of discovery, the licensee shall document and track
    1. Any failure, compromise, degradation, or discovered vulnerability in a cyber security control applied to an identified asset; or
    2. A cyber attack that compromises an identified asset associated with a latent consequence of concern for control and accounting of special nuclear material and strategic special nuclear material.

9. Records
    a. Retain all supporting technical documentation demonstrating compliance with the requirements of this section as a record.
    b. Maintain all records required to be kept by Commission regulations, orders, or license conditions until the Commission terminates the license for which the records were developed.
    c. Maintain superseded records for at least three (3) years, unless otherwise specified by the Commission.