DRAFT PROPOSED RULE TEXT

§ 73.53 Requirements for cyber security at nuclear fuel cycle facilities.

(a) *Applicability.* The requirements of this section apply to each applicant or licensee subject to the requirements of 10 CFR 70.60 and each applicant or licensee of a uranium hexafluoride conversion or deconversion facility licensed under 10 CFR Part 40, "Domestic Licensing of Source Material." By [date], each current licensee shall submit, as an amendment to its license, a cyber security plan that satisfies the requirements of this section for Commission review and approval. Each applicant who has submitted an application to the Commission prior to the effective date of this rule must amend the application to include a cyber security plan that satisfies the requirements of this section for Commission review and approval. The cyber security plan must be fully implemented by the date specified in the Commission's written approval of the license or plan.

(b) *Cyber security program performance objectives.* The applicant or licensee shall establish, implement, and maintain a cyber security program to prevent a cyber attack from causing a consequence of concern as identified in paragraph (c) of this section. The program shall:

(1) Protect vital digital assets using the cyber security controls described in paragraph (d)(2) of this section.

(2) Detect cyber attacks associated with a consequence of concern.

(3) Respond to cyber attacks associated with a consequence of concern.

(4) Recover from cyber attacks associated with a consequence of concern.

(c) *Consequences of concern.* The licensee's cyber security program shall be designed to protect against active and latent consequences of concern.

(1) *Active consequences of concern – safety.* One or more of the following consequences that directly results from a cyber attack:

(i) A radiological exposure of:

(A) 25 rem or greater for any individual; or

(B) 30 mg or greater intake of uranium in soluble form for any individual outside the controlled area; or

(ii) An acute chemical exposure that could lead to irreversible or other serious, long lasting health effects for any individual.

(2) *Latent consequences of concern – safety and security.* The compromise, as a result of a cyber attack, of a function needed to prevent, mitigate, or respond to one or more of the following:

(i) A radiological exposure of:

(A) 25 rem or greater for any individual; or

(B) 30 mg or greater intake of uranium in soluble form for any individual outside the controlled area; or

(ii) An acute chemical exposure that could lead to irreversible or other serious, long lasting health effects for any individual; or

(iii) Loss or unauthorized disclosure of classified information or classified matter.

(3) *Latent consequences of concern – safeguards.* The compromise, as a result of a cyber attack at a licensee authorized to possess or use special nuclear material of moderate strategic significance, of a function needed to prevent, mitigate, or respond to one or more of the following:

(i) Unauthorized removal of special nuclear material of moderate strategic significance as specified in 10 CFR 73.67(d); or

(ii) Loss of nuclear material control and accounting for special nuclear material of moderate strategic significance as specified in 10 CFR 74.41(a).

(4) *Latent consequences of concern – design basis threat.* The compromise, as a result of a cyber attack at a licensee authorized to possess or use a formula quantity of strategic special nuclear material, of a function needed to prevent, mitigate, or respond to one or more of the following:

(i) Radiological sabotage, as specified in 10 CFR 73.1(a)(1);

(ii) Theft or diversion of formula quantities of strategic special nuclear material, as specified in 10 CFR 73.1(a)(2); or

(iii) Loss of nuclear material control and accounting for strategic special nuclear material, as specified in 10 CFR 74.51(a).

(d) *Cyber security program.* To meet the performance objectives in paragraph (b) of this section, the licensee shall:

(1) Establish and maintain a Cyber Security Team responsible for the execution of the cyber security program. The Cyber Security Team shall include a management structure that provides oversight of the cyber security program. The Cyber Security Team shall be adequately staffed, trained, qualified, and equipped.

(2) Establish and maintain a set of cyber security controls for each applicable consequence of concern identified in paragraph (c) of this section. The cyber security controls shall address access control, audits and accountability, awareness and training, configuration management, contingency planning, identification and authorization, incident response, maintenance, media protection, physical and environmental protection, planning, program management, security assessments and authorization, system and communication protection, system and information integrity, and system service acquisition.

(3) Identify digital assets and associated support systems:

(i) That if compromised by a cyber attack, would directly result in an active consequence of concern identified in paragraph (c)(1) of this section.

(ii) That if compromised by a cyber attack, would result in a latent consequence of concern identified in paragraphs (c)(2)-(4) of this section.

(iii) The licensee need not identify digital assets that are a part of a classified system approved or accredited by another Federal agency.

(4) Determine which digital assets, identified through paragraph (d)(3) of this section, are vital. A digital asset is vital if:

(i) It is identified through paragraph (d)(3)(i) of this section, and no alternate means protected from a cyber attack can be credited to prevent the active consequence of concern; or

(ii) It is identified through paragraph (d)(3)(ii) of this section, and no alternate means protected from a cyber attack can be credited to maintain the function needed to prevent, mitigate, or respond to the latent consequence of concern.

(5) Conduct validation testing for each vital digital asset identified through paragraph (d)(4) of this section.

(6) Establish and maintain written implementing procedures for the application of cyber security controls to vital digital assets. These procedures shall:

(i) Document the applicable cyber security controls for each vital digital asset, using the sets of cyber security controls identified through paragraph (d)(2) of this section;

(ii) Specify appropriate values for cyber security control parameters; and

(iii) Provide for interim compensatory measures to meet the cyber security program performance objectives when cyber security controls are degraded. When implemented, interim compensatory measures must be documented, tracked to completion, and available for inspection by NRC staff.

(e) *Cyber security plan.* The licensee shall establish, implement, and maintain a cyber security plan that describes how the cyber security program performance objectives in paragraph (b) of this section are met.

(1) In developing the cyber security plan, the licensee must identify and analyze site-specific conditions that impact the implementation and maintenance of the cyber security program.

(2) The cyber security plan must describe the cyber security controls established through paragraph (d)(2) of this section.

(3) The cyber security plan must include measures for incident response and recovery from a cyber attack affecting vital digital assets identified through paragraph (d)(4) of this section. The incident response and recovery measures must, at a minimum:

(i) Maintain the capability for timely detection of and response to the cyber attack;

(ii) Prevent or mitigate the impacts of a consequence of concern; and

(iii) Identify and correct cyber security vulnerabilities.

(4) Policies, implementing procedures, site-specific analysis, and other supporting technical information used by the licensee to support the development and implementation of the cyber security plan need not be submitted for Commission review and approval as part of the cyber security plan but are subject to inspection by the NRC staff.

(f) *Configuration management.* The licensee shall ensure that any previously unidentified digital assets or modifications affecting existing digital assets identified through paragraph (d)(3) of this section, are evaluated prior to operating and the cyber security program performance objectives in paragraph (b) of this section are met.

(g) *Biennial review of the cyber security program.* The licensee shall perform a review of the cyber security program at least every 24 months. This review must document, track, and address in a timely manner findings, deficiencies, and recommendations that result from:

(1) An analysis of the effectiveness and adequateness of the program;

(2) A review of the procedures implementing cyber security controls; and

(3) A vulnerability evaluation of the digital assets identified through paragraph (d)(3) of this section and their associated cyber security controls, alternate means of protection, and defensive architecture.

(h) *Event reporting and tracking.* The licensee shall make notifications as required under existing regulations and shall, when known, inform the NRC that the notification is a result of a cyber attack. In addition, the licensee shall document within 24 hours of discovery and track to resolution the following:

(1) Any failure, compromise, degradation, or discovered vulnerability in a cyber security control implemented through paragraph (d)(6) of this section; or

(2) A cyber attack that compromises a vital digital asset associated with a consequence of concern described in paragraphs (c)(3)(ii) and (c)(4)(iii) of this section.

(i) *Records.* The licensee shall retain all supporting technical documentation demonstrating compliance with the requirements of this section as a record. The licensee shall maintain and make available for inspection all records, reports, and documents required to be

kept by Commission regulations, orders, or license conditions until the Commission terminates the license. The licensee shall maintain superseded portions of these records, reports, and documents for at least 3 years after they are superseded, unless otherwise specified by the Commission.