[NOTE: The following document contains change bars along the left border to indicate revised text implemented since the previouse published version on May 19, 2016, (i.e., Agencywide Documents Access and Management System no. – ML16131A115). To facilitate readability, revised text is marked red and underlined; deleted text has been removed.]

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

(a) *Introduction*. 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 THAT IS 180 DAYS AFTER THE DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, each current licensee shall submit, through an application for amendment of 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 **[DATE THAT IS 30 DAYS AFTER THE DATE OF PUBLICATION IN THE FEDERAL REGISTER],** 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 that shall detect, protect against, and respond to a cyber attack capable of causing a consequence of concern as identified in paragraph (c) of this section.

(c) *Consequences of concern.* The licensee's cyber security program shall be designed to protect against the following four types of consequences of concern.

(1) *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 §73.1(a)(1);

(ii) Theft or diversion of formula quantities of strategic special nuclear material, as specified in §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).

(2) *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 §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).

(3) *Active consequences of concern – safety.* One or more of the following 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.

(4) *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.

(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 that is adequately structured, staffed, trained, qualified, and equipped to implement the cyber security program.

(2) Establish and maintain cyber security controls that provide the capability to prevent a cyber attack from causing a consequence of concern. These cyber security controls shall be specific to each of the applicable types of consequences of concern identified in paragraph (c) of this section.

(3) Identify digital assets that if compromised by a cyber attack, would result in a consequence of concern identified in paragraph (c) of this section. The licensee does not need to identify digital assets that are a part of a classified system accredited or authorized by another Federal agency under a formal security agreement with NRC.

(4) Determine which digital assets, identified through paragraph (d)(3) of this section, and associated support systems are vital. A digital asset is vital if no alternate means that is protected from a cyber attack can be credited to prevent the active consequence of concern or maintain the function needed to prevent, mitigate, or respond to the latent consequence of concern.

(5) Ensure that each vital digital asset is protected against a cyber attack by:

(i) Applying the applicable cyber security controls identified through paragraph (d)(2) of this section; and

(ii) Establishing and maintaining written implementing procedures documenting the countermeasures to a cyber attack taken to address the cyber security controls.

(6) When the countermeasures to a cyber attack taken to address the cyber security controls are degraded, provide interim compensatory measures to meet the cyber security program performance objectives. 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 accounts for site specific conditions and describes how the cyber security program performance objectives in paragraph (b) of this section are met.

(1) The cyber security plan must document the program requirements established and maintained through paragraphs (d)(1) and (2) of this section.

(2) The cyber security plan must describe measures for:

(i) Management and performance of the cyber security program; and

(ii) Incident response to a cyber attack affecting vital digital assets.

(3) 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 each change to the facility, including modification of an existing digital asset identified through paragraph (d)(3) of this section, is evaluated prior to implementation and does not adversely impact the licensee's ability to meet the cyber security program performance objectives in paragraph (b) of this section.

(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) Verification of the effectiveness and adequateness of the program;

(2) Review of the implementing procedures for cyber security controls; and

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

(h) *Event reporting and tracking.* The licensee shall inform the NRC upon discovery that an event requiring notification under existing regulations is the result of a cyber attack. In addition, the following shall be recorded within 24 hours of discovery and tracked to resolution:

(1) A failure, compromise, degradation, or discovered vulnerability in a cyber security control implemented through paragraph (d)(5) of this section; or

(2) A cyber attack that compromises a vital digital asset associated with a consequence of concern described in paragraphs (c)(1)(ii) and (2)(iii) of this section.

(i) *Records.* The licensee shall retain 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.