§ 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 Title 10 of the *Code of Federal Regulations* 10 CFR Part 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 must 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 must establish, implement, and maintain a cyber security program that will 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 must 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 facility of a licensee authorized to possess or use a formula quantity of strategic special nuclear material, of a function needed to prevent 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 facility of a licensee authorized to possess or use special nuclear material of moderate strategic significance, of a function needed to prevent 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 25 rem or greater for any individual;

(ii) An intake of 30 mg or greater of uranium in soluble form 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.

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

(i) A radiological exposure of 25 rem or greater for any individual;

(ii) An intake of 30 mg or greater of uranium in soluble form 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; or

(iv) 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 must:

(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 performance specifications to detect, protect against, and respond to a cyber attack capable of causing a consequence of concern. These cyber security controls must 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 consequence of concern.

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

(i) Identifying the cyber security controls, established through paragraph (d)(2) of this section, applicable to the type of consequence of concern associated with the vital digital asset; and

(ii) Establishing and maintaining written implementing procedures documenting the measures taken to address the performance specifications associated with the identified cyber security controls.

(6) When the measures 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 must 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 describe how the licensee will:

(i) Satisfy the requirements of this section;

(ii) Manage the cyber security program; and

(iii) Provide cyber security incident response to a cyber attack capable of causing a consequence of concern.

(2) Policies, implementing procedures, site-specific analyses, 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 but must be documented and available for inspection by NRC staff.

(f) *Configuration management.* The licensee must utilize a configuration management system to ensure that changes to the facility, including modification of an existing digital asset identified through paragraph (d)(3) of this section, are evaluated prior to implementation and do not adversely impact the licensee's ability to meet the cyber security program performance objectives in paragraph (b) of this section. This system must be documented in written procedures available for inspection by NRC staff.

(g) *Review of the cyber security program.*

(1) Licensees authorized to possess or use a formula quantity of strategic special nuclear material must perform a review of the cyber security program as a component of the security program in accordance with the requirements of §73.46(g)(6).

(2) All other licensees must perform a review of the cyber security program at least every 36 months.

(i) The review must include an audit of the effectiveness and adequacy of the cyber security program including, but not limited to:

(A) Implementing procedures; and

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

(ii) The findings, deficiencies, and recommendations resulting from the review must be:

(A) Tracked and addressed in a timely manner; and

(B) Documented in a report to the licensee's plant manager and to corporate management at least one level higher than that having responsibility for day-to-day plant operations.

(h) *Event reporting and tracking.*

(1) The licensee must inform the NRC Operations Center within 1 hour of discovery that an event requiring notification under existing regulations is the result of a cyber attack.

(2) The licensee must record, within 24 hours of discovery, and track to resolution the following:

(i) A failure, compromise, discovered vulnerability, or degradation that results in a decrease in effectiveness of a cyber security control identified through paragraph (d)(5) of this section; or

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

(3) The items recorded through paragraph (h)(2) of this section need not be reported to the NRC Operations Center but must be documented and available for inspection by the NRC staff.

(i) *Records.* The licensee must retain supporting technical documentation demonstrating compliance with the requirements of this section as a record. The licensee must 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 must maintain superseded portions of these records, reports, and documents for at least 3 years after they are superseded, unless otherwise specified by the Commission.