Draft Environmental Assessment and Finding of No Significant Impact for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR 73.53)

RIN number: 3150-AJ64

NRC Docket ID: NRC-2015-0179

2017

INTRODUCTION

The U.S. Nuclear Regulatory Commission (NRC) is proposing to amend its regulations in Part 73 of Title 10 of the *Code of Federal Regulations* (10 CFR), "Physical Protection of Plants and Materials," to add cyber security requirements for certain nuclear fuel cycle facility (FCF) applicants and licensees. The proposed regulation, if approved, would require FCF applicants and licensees within the scope of the rule to establish, implement, and maintain a cyber security program designed to promote common defense and security and to provide reasonable assurance that the public health and safety remain adequately protected against the evolving risk of cyber attacks. The proposed rule would apply to each applicant or licensee subject to 10 CFR 70.60, "Applicability," and to each applicant or licensee subject to the requirements of 10 CFR Part 40, "Domestic Licensing of Source Material," for the operation of a uranium hexafluoride conversion or deconversion facility (hereafter FCF licensees).

HISTORICAL BACKGROUND AND OVERVIEW

Certain NRC-licensed FCFs are subject to either the design basis threats (DBTs) described in 10 CFR 73.1 or to the Interim Compensatory Measures (ICM) Orders issued to all FCF licensees in 2002 and 2003. Both the DBTs and the ICM orders require consideration of a cyber attack when evaluating security vulnerabilities. However, the NRC's current physical protection regulations in 10 CFR Part 73 do not provide specific requirements on how to implement these performance objectives. For example, there are no regulatory requirements for FCF licensees to analyze, identify, or protect digital assets that could be compromised by a cyber attack.

The cyber threat, including the number of cyber adversaries and the types of attack methods and vectors, has evolved in scope and complexity since the ICM Orders were issued and the DBTs were revised. The NRC staff has observed that cyber attacks have exploited security vulnerabilities at global critical infrastructure facilities similar to the security vulnerabilities staff has documented at NRC-licensed FCFs. Exploitation of these vulnerabilities at an NRC-licensed FCF could compromise existing digital assets necessary to prevent one of the consequences of concern defined in the proposed rule.

In addition, the safety provisions for FCF licensees contained in 10 CFR Part 20, "Standards for Protection Against Radiation," Part 40, and Part 70, "Domestic Licensing of Special Nuclear Material," do not require licensees to consider threats from cyber attacks. As required by Part 70, Subpart H, "Additional Requirements for Certain Licensees Authorized to Possess a Critical Mass of Special Nuclear Material," certain FCF licensees must evaluate specific performance requirements through an integrated safety analysis, but they are not required to consider malicious acts. Therefore, the safety regulatory requirements and their associated guidance documents do not provide a regulatory framework to protect against cyber attacks.

Given the evolution in the cyber threat to FCF licensees since the ICM Orders were issued and the DBTs were revised, the NRC staff has determined that specific cyber security requirements for FCF licensees are warranted. In the staff requirements memorandum (SRM) for SECY-14-0147, "Cyber Security for Fuel Cycle Facilities," dated March 24, 2015 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML15083A175), the Commission directed the staff to proceed with a high priority cyber security rulemaking for FCFs and to complete and implement the final rule in an expeditious manner.

ENVIRONMENTAL ASSESSMENT

I. Identification of the Proposed Action

The proposed action is the adoption of new requirements in 10 CFR 73.53, "Requirements for cyber security at nuclear fuel cycle facilities," with conforming changes in 10 CFR Parts 40, 70, and 73. The proposed requirements would apply to each FCF licensee that is or plans to be authorized to: (1) possess greater than a critical mass of special nuclear material (SNM) and engage in enriched uranium processing, fabrication of uranium fuel or fuel assemblies, uranium enrichment, enriched uranium hexafluoride conversion, plutonium processing, fabrication of mixed-oxide fuel or fuel assemblies, scrap recovery of SNM, or any other FCF activity that the Commission determines could significantly affect public health and safety; or (2) engage in uranium hexafluoride conversion or uranium hexafluoride deconversion. As such, the proposed rule would apply to FCF licensees subject to 10 CFR 70.60 and FCF licensees subject to 10 CFR Part 40 for operation of a uranium hexafluoride conversion or deconversion facility.

If adopted, FCF licensees would be required to establish, implement, and maintain a cyber security program to detect, protect against, and respond to a cyber attack capable of causing a consequence of concern. The proposed provisions of 10 CFR 73.53 would require that FCF licensees implement a comprehensive cyber security program. Paragraph (a) would identify the licensees and applicants for which the requirements apply, and require these licensees and applicants to submit a cyber security plan for NRC review and approval. Paragraph (b) would set forth the program performance objectives to detect, protect against, and respond to a cyber attack capable of causing a consequence of concern. Paragraph (c) would establish the four types of consequences of concern that licensee cyber security programs must protect against

and would also define the safety, security, and safeguards thresholds for each of those consequences of concern. Paragraph (d) would establish the required elements of a licensee's cyber security program, including formation of a cyber security team, identification of vital digital assets (VDAs), and the application of cyber security controls to VDAs in accordance with implementing procedures. Paragraph (e) would identify the requirements to develop and maintain a cyber security plan that describes the cyber security program. Paragraph (f) would require licensees to use a configuration management system to keep the cyber security program up to date and apply temporary compensatory measures to new conditions. Paragraph (g) would require licensees to perform periodic reviews of the cyber security program. Paragraph (h) would require cyber security event reporting and tracking. Paragraph (i) would establish recordkeeping requirements.

II. Need for the Action

As described in Section I of this assessment, the proposed rule would define requirements for a cyber security program that is needed to prevent a consequence of concern. The NRC staff has determined that those parts of the proposed rule that are designed to prevent security and safeguards consequences of concern are necessary to promote common defense and security and to provide reasonable assurance that the public health and safety remain adequately protected against the evolving risk of cyber attacks. Furthermore, the staff has determined that those parts of the proposed rule that are designed to protect against the safety consequences of concern provide a substantial increase in overall protection of the public health and safety at FCFs. Additional discussion of these issues is provided in the backfit analysis for the proposed rule, "Draft Backfit Analysis and Documented Evaluation for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR 73.53)" (ADAMS Accession No. ML17018A221).

III. Alternatives to the Proposed Action

In addition to the proposed action, the NRC staff considered the alternative of taking no action. Implementation of the proposed rule is the only option that completely resolves the regulatory issues identified in Section II of this assessment

Alternative 1: No Action

The no action alternative would maintain the NRC's current approach to cyber security at FCFs. Under this option, the NRC would not modify 10 CFR Part 73. The only cyber security requirements for FCF licensees would be those in the 2002-2003 ICM Orders and, for Category I FCF licensees, the requirement to protect against a cyber attack as part of the DBT defined in 10 CFR 73.1(a).

The alternative of taking no action would avoid the costs that the proposed rule would impose. However, the no action alternative does not address the evolving cyber security threat discussed in Section II and in the draft regulatory analysis, "Draft Regulatory Analysis for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR 73.53)" (ADAMS Accession No. ML16320A452), developed as part of this rulemaking. Therefore, the no action alternative would not ensure that FCFs remain adequately protected from a cyber attack. For these reasons, the NRC staff does not recommend the no action alternative.

Other Approaches Considered

In developing the proposed rule, the NRC staff considered a number of additional approaches to improving cyber security for FCF licensees, including issuing generic communications, developing new guidance documents, and revising existing inspection modules or enforcement guidance. Because these approaches would not establish a regulatory framework and specific requirements addressing the safety and security issues described in Section II and the draft regulatory analysis, the staff did not evaluate them as alternatives to the proposed action, and therefore, this environmental assessment does not contain an evaluation of the environmental impacts of these approaches.

In SECY-14-0147, the NRC staff presented the Commission with an option to issue orders imposing cyber security requirements on FCF licensees. The staff provided a draft security order that would have required that FCF licensees: create a cyber security team, conduct awareness training, establish an incident response capability to a cyber attack, implement portable media controls, perform a baseline inventory of digital assets, isolate specific assets, develop applicable configuration management controls, and report certain events.

In the SRM for SECY-14-0147, the Commission did not support the issuance of orders and directed the NRC staff to proceed directly with a high priority rulemaking. Based on the Commission's direction, the staff has not considered the issuance of orders as an alternative. Accordingly, this environmental assessment does not contain an evaluation of the environmental impacts of issuing orders.

Summary of Alternatives to the Proposed Action

The NRC staff considered the no action alternative and determined that it has disadvantages when compared to the option involving issuance of a proposed rule. The proposed rule would implement a graded, consequence-based approach at FCFs for the protection of digital assets from a cyber attack capable of causing a consequence of concern. It would also improve regulatory stability by establishing comprehensive cyber security requirements for FCF licensees. Additionally, the proposed rule would enable the NRC to develop an effective inspection program, reduce regulatory uncertainty, and address enforceability issues. The staff concludes that the proposed rule is the preferred action because it would promote clarity, effectiveness, and openness in the regulatory process by providing an open and transparent cyber security regulatory framework that FCF licensees can consistently implement.

Environmental Impacts of the Proposed Action and Alternative

In accordance with 10 CFR Part 51, "Environmental Protection Regulations for Domestic Licensing and Related Regulatory Functions," this environmental assessment includes an evaluation of any potential effects that the proposed rule may have on the environment. This proposed action would impose new cyber security requirements on FCF licensees, as summarized in Section I of this assessment. As discussed in the following paragraphs, the NRC staff has concluded that there would not be any significant radiological or non-radiological environmental impacts associated with implementation of the proposed cyber security rule requirements.

The proposed security requirements address cyber security at FCFs and would not adversely affect licensees' systems that limit the release of radiological effluents. Rather, the safety, security, and safeguards functions provided by these systems would potentially be enhanced by the proposed action. The proposed cyber security requirements are designed to ensure that safety, security, and safeguards systems are protected and not compromised through a cyber attack. As such, the proposed requirements would enhance safety and security by protecting digital assets performing safety, security, and safeguards functions from a cyber attack. Thus, there are no significant radiological effluent impacts associated with this action.

The standards and requirements applicable to radiological releases and effluents are not affected by the proposed rule and continue to apply to the affected equipment, facilities, and procedures. In addition, the proposed action would not increase the probability or consequences of accidents involving an occupational exposure to radiation. Therefore, there would be no significant increase in occupational exposure as a result of this action. Furthermore, the proposed action would not increase the probability or consequences of accidents, nor would it result in changes to the types of any effluents that may be released offsite that could result in public exposure to radiation. Therefore, there would be no significant increase in public exposure as a result of this action.

With regard to potential non-radiological impacts, the NRC staff concluded that implementation of this proposed rule would not have a significant impact on the environment. No major construction of new structures is required to meet the requirements in the proposed rule. Therefore, facility footprints should not change due to the proposed action. In addition, implementation of the proposed rule would not affect any historic site or non-radiological

effluents. Therefore, there is no significant non-radiological environmental impact associated with this action.

For the reasons discussed above, the NRC staff concludes that there would be no significant environmental impact associated with the proposed rule.

Environmental Impacts of Alternatives to the Proposed Action

As an alternative to the proposed rule, the NRC staff considered not taking any action with respect to revising the security regulations. This would result in no change to the current environmental impacts.

IV. Agencies and Persons Consulted

No agencies or persons outside the NRC were contacted in connection with the preparation of this draft environmental assessment. The NRC is requesting comments on the draft environmental assessment as a part of the proposed rule process.

FINDING OF NO SIGNIFICANT IMPACT

The NRC staff has determined under the National Environmental Policy Act of 1969, as amended, and the NRC's regulations in Subpart A of 10 CFR Part 51, that the proposed amendments are not a major Federal action significantly affecting the quality of the human

environment, and therefore, an environmental impact statement is not required. The proposed amendments would establish cyber security requirements for FCF licensees and would have no significant impact on the human environment.

The determination of this environmental assessment is that there will be no significant impact to the human environment from this action. However, the general public should note that the NRC staff welcomes public participation. Comments on any aspect of this Environmental Assessment may be submitted to: Secretary, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, Attn: Rulemakings and Adjudications Staff, Docket ID NRC-2015-0179.