Evaluation of Fuel Cycle Facilities

On June 12, 2014, the U.S. Nuclear Regulatory Commission (NRC) received a petition for rulemaking (PRM) from Anthony Pietrangelo on behalf of the Nuclear Energy Institute (Agencywide Documents Access and Management System (ADAMS) Accession No. ML14184B120). The NRC assigned docket number PRM-73-18 to this petition and published a notice of receipt and opportunity to comment in the *Federal Register* on September 22, 2014 (79 FR 56525; September 22, 2014).

The focus of PRM-73-18 is specific to the NRC's cyber security regulations for power reactors in Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54. However, the NRC staff made a commitment in SECY-17-0099, "Proposed Rule – Cyber Security at Fuel Cycle Facilities" (ADAMS Accession No. ML17018A218), to determine if any corresponding changes are necessary to the fuel cycle facility (FCF) proposed rule resulting from the disposition of PRM-73-18. The proposed rule, which is currently before the Commission, if approved would require certain FCF applicants or licensees to establish, implement, and maintain a cyber security program. In keeping with this commitment in SECY-17-0099, the staff has evaluated the assertions made by the petitioner in PRM-73-18 and, for the reasons discussed below, has determined that they do not raise any issues that would require changes to FCF cyber security proposed rule.

The petitioner raised two issues in PRM-73-18 supported by several additional assertions. First, the petitioner argues that the language in 10 CFR 73.54(a) is inconsistent with the original intent of the cyber security rule to only require protection of those computer systems and networks that if compromised could directly result in significant core damage or spent fuel sabotage. Second, the petitioner argues that the broad scoping language in 10 CFR 73.54(a)(1) unnecessarily requires licensees to expend time, resources, and costs for the protection from a cyber-attack for those digital assets not directly related to preventing radiological sabotage.

The analysis below examines the petitioner's assertions in support of the premise that the language in the power reactor cyber security rule (i.e., 10 CFR 73.54(a)) is overly broad and therefore requires the protection of digital computer systems and networks that do not have a nexus to radiological sabotage and is therefore not justified. For the reasons discussed in detail below, the NRC staff has determined that the assertions in PRM-73-18 do not raise any issues that would warrant changes to the FCF cyber security proposed rule. However, through ongoing engagements with stakeholders, the staff has become aware of one issue that may benefit from stakeholder input during the comment period. This issue is discussed more fully below.

Background

The NRC has tailored the various cyber security requirements in 10 CFR to align with the respective licensing basis applicable to each category of licensees. Regulatory requirements are uniform across various categories of licensees only so far as those requirements are justifiable through risk-informed, performance-based considerations established through the regulatory bases for those requirements. All FCF licensees are subject to the Interim Compensatory Measure (ICM) Orders issued in 2002 and 2003 and are therefore required to consider both physical and cyber security vulnerabilities in the design of their protective strategies. However, the NRC's regulatory structure does not set forth specific cyber security requirements or guidance on how these vulnerabilities should be addressed. Furthermore, the

Design Basis Threats (DBT) in 10 CFR 73.1(a)(1)(E)(v) & (2)(E)(v) also include a cyber-attack as an attribute that licensees must protect against but do not provide specific requirements for licensees to analyze, identify, or protect digital assets. The proposed rule for cyber security at FCFs would address these regulatory gaps by providing performance objectives to protect against cyber-attacks capable of causing specific consequences of concern. Also, the proposed rule provides graded requirements to codify the cyber considerations from the ICM Orders and DBTs to protect against cyber-attacks. Protecting against the proposed rule's consequences of concern will enable FCF licensees to accomplish the security performance objectives in, for example, the ICM Orders and 10 CFR Part 73 that are applicable to each specific type of facility.

The proposed rule for cyber security at FCFs would apply a graded, consequence-based approach to the protection of digital assets that takes into account hazards specific to the different facility types of FCF licensees. These licensees include: (1) 10 CFR Part 70 licensees authorized to possess or use a formula quantity of strategic special nuclear material (SSNM) as defined in 10 CFR 73.2, "Definitions" (Category I FCF licensees); (2) 10 CFR Part 70 licensees authorized to possess or use special nuclear material (SNM) of moderate strategic significance as defined in 10 CFR 73.2 (Category II FCF licensees); (3) 10 CFR Part 70 licensees authorized to possess or use SNM of low strategic significance as defined in 10 CFR 73.2 (Category III FCF licensees); and (4) 10 CFR Part 40 licensees authorized to perform uranium hexafluoride conversion or deconversion (conversion or deconversion facility licensees). Under this graded, consequence-based approach, FCF licensees would only have to protect against the defined consequences of concern applicable to their specific type of facility as defined in the proposed rule for cyber security at FCFs.

NRC Staff Evaluation of Petitioner's PRM-73-18 Assertions in the Context of SECY-17-0099

Petitioner's Assertion A in PRM-73-18 states that the NRC's cyber security rule language in 10 CFR 73.54(a) was changed from the original language in the proposed rule without public notice and comment. It further states that the implications of this change were not clearly understood at the time the change was made. This assertion is not applicable to the FCF cyber security proposed rule that is currently under review by the Commission. If the Commission approves the FCF cyber security proposed rule, the language of the proposed rule will be made available for public notice and comment.

Similarly, Petitioner's Assertion E in PRM-73-18 argues that violations of the NRC's power reactor cyber security requirements identified during NRC inspections illustrate the problems created by the broad scoping language in 10 CFR 73.54. Although SECY-17-0099 incorporates lessons learned from the inspections referenced by the petitioner in Assertion E, the FCF cyber security rule has not been approved by the Commission, and therefore it has not been implemented by licensees and no inspections have occurred. Accordingly, petitioner's Assertion E is not applicable to the FCF cyber security proposed rule. As discussed more fully below in response to other petitioner assertions, the NRC staff has determined that the scope of FCF cyber security proposed rule is appropriate.

The NRC staff also evaluated petitioner's Assertions B – D in PRM-73-18 to determine if they raise any issues that could be relevant to the FCF cyber security proposed rule in SECY-17-0099. The NRC staff's evaluation of Assertions B – D are below.

Discussion of the Applicability of Petitioner's PRM-73-18 Assertion B to SECY-17-0099

Petitioner's Assertion B in PRM-73-18 argues that the language in 10 CFR 73.54(a)(1) enlarges the scope of digital assets to be protected from cyber-attack beyond what the Commission originally intended. The petitioner asserts that this has created an inconsistency between the NRC's power reactor cyber security requirements and the performance objectives of 10 CFR 73.55, and results in the protection of digital assets that have no relationship to protecting against radiological sabotage.

Consequences of Concern at Fuel Cycle Facilities

The proposed rule for cyber security at FCFs would require licensees to identify digital assets that potentially require protection by establishing four types of consequences of concern that an FCF licensee's cyber security program would need to protect against: (1) latent consequences of concern – DBT; (2) latent consequences of concern – safeguards; (3) active consequences of concern – safety; and (4) latent consequences of concern – safety and security. These consequences of concern consider the licensing basis and characteristics of various types of FCFs while providing an appropriate graded, consequence-based approach applicable to digital assets (called vital digital assets) requiring protection at each type of facility.

The consequences of concern in the proposed rule for FCFs recognize two general types of effects that a cyber-attack can cause (i.e., active and latent consequences of concern). There are distinct differences between active and latent consequences of concern. In the case of an active consequence of concern, the compromise of the digital asset from a cyber-attack directly results in a radiological or chemical exposure exceeding the regulatory thresholds set forth in the proposed rule. In the case of a latent consequence of concern, a digital asset is compromised but there is no direct impact on a safety, security, or safeguards function until a secondary event occurs (i.e., an initiating event separate from the cyber-attack).

The petitioner has asserted that the NRC's cyber security rule for power reactors requires the protection of digital assets that have no nexus to radiological safety because they cannot directly cause significant core damage or spent fuel sabotage even if compromised (i.e., Petitioner's Assertion B). During the development of SECY-17-0099, the NRC staff drafted proposed rule language that establishes appropriate thresholds for consequences of concern for each category of FCF licensee, taking into account their specific characteristics and licensing basis. Given this focus in the proposed rule language, the NRC staff has determined that the FCF cyber security proposed rule only requires protection of appropriate digital assets at each type of FCF facility. The discussion in each of the subsections below provides the NRC staff's evaluation of the specific thresholds for each of the consequences of concern.

Latent consequences of concern – DBT

A latent consequence of concern – DBT would only be applicable to an FCF authorized to possess or use a formula quantity of SSNM (i.e., a Category I FCF). Consistent with protecting against the DBTs, a Category I FCF licensee is required to prevent radiological sabotage (i.e., 10 CFR 73.1(a)); theft or diversion of formula quantities of SSNM (i.e., 10 CFR 73.1(a)(2)); or the loss of material control and accounting for the SSNM (i.e., 10 CFR 74.51(a)). This is unlike power reactor licensees, which are required to protect against the single DBT to prevent radiological sabotage (i.e., 10 CFR 73.1(a)). A latent consequence of concern – DBT involves the compromise, because of a cyber-attack, of a digital asset performing a security or safeguards function. The result is that the function cannot be relied upon when required.

The Draft Backfit Analysis (Agencywide Documents Access and Management System (ADAMS) Accession No. ML17018A221) for SECY-17-0099 provides further evaluation regarding the latent consequence of concern – DBT. The NRC staff does not recommend any changes to the scope of this provision of the proposed rule as a result of the assertions made by the petitioner in PRM-73-18.

Latent consequences of concern – safeguards

A latent consequence of concern – safeguards would only be applicable to an FCF authorized to possess or use SNM of moderate strategic significance (i.e., Category II FCF). This consequence of concern involves the compromise, as a result of a cyber-attack, of a digital asset performing a security function which would allow a malicious actor to exploit the degraded security function that was put in place to prevent the unauthorized removal of SNM of moderate strategic significance (10 CFR 73.67(d)) or the loss of material control and accounting for SNM of moderate strategic significance (10 CFR 74.41(a)). The result is that the security function cannot be relied upon when required.

The latent consequence of concern – safeguards protects against a unique concern at Category II FCFs that is not present at power reactors. The NRC staff does not recommend any changes to the scope of this provision of the proposed rule as a result of the assertions made by the petitioner in PRM-73-18.

Active consequences of concern – safety

An active consequence of concern (safety) may be directly caused by a cyber-attack. In this situation, the cyber-attack compromises the function of a digital asset and directly leads to one or more of the following safety-related consequences: radiological exposure of 0.25 Sv (25 rem) or greater for any individual; intake of 30 mg or greater of uranium in soluble form for any individual outside the controlled area; or an acute chemical exposure that could lead to irreversible or other serious, long lasting health effects for any individual.

The thresholds for the safety consequences of concern in SECY-17-0099, include both on-site and off-site consequences, which are consistent with the performance requirements in 10 CFR 70.61. Inadvertent criticalities and significant chemical exposures are hazards that are unique to FCFs and result in on-site consequences. A cyber-attack leading to an inadvertent criticality at an FCF would be a significant on-site radiological event, but generally have little physical impact off-site. Similar radiological and chemical events, having potentially significant on-site consequences with little off-site consequences, have a much lower likelihood at power reactors. Further consideration of on-site personnel in the proposed rule for cyber security at FCFs is included below, in the discussion of Petitioner's Argument D.

Providing protection from chemical consequences resulting from a cyber-attack aligns with the Department of Homeland Security's (DHS's) Chemical Facility Anti-Terrorism Standards (CFATS) set forth in 6 CFR Part 27. These standards require protection from cyber-attacks that could create a toxicity, flammability, or explosion hazard that would affect populations within and beyond a facility. Although facilities where NRC imposes significant requirements and regulates safety and security are given a statutory exemption from DHS's CFATS requirements, the proposed safety consequences of concern are consistent with overall approach of DHS's requirements for similar chemical facilities. Moreover, the need for protection from chemical consequences differs between fuel cycle facilities and power reactor facilities due to the amount of chemicals at the facilities and the differences in the resultant consequences of concern.

The NRC staff does not recommend any changes to the scope of this provision of the proposed rule as a result of the assertions made by the petitioner in PRM-73-18.

Latent consequences of concern – safety or security

A latent consequence of concern (safety or security) involves the compromise of a safety or security function due to a cyber-attack. In this situation, the cyber-attack renders a digital asset incapable of performing its intended function. When called upon to respond to an event, separate from the cyber-attack, the digital asset does not operate as expected, and therefore the supported safety or security function is compromised, resulting in one or more of the following consequences of concern: radiological exposure of 0.25 Sv (25 rem) or greater for any individual; intake of 30 mg or greater of uranium in soluble form for any individual outside the controlled area; acute chemical exposure that could lead to irreversible or other serious, long-lasting health effects for any individual; or loss or unauthorized disclosure of classified information or classified matter (i.e., 10 CFR Part 95). The safety considerations for the thresholds of this consequence of concern are identical to those provided within the subsection above on the active consequence of concern – safety. The NRC staff does not recommend any changes to the scope of this provision of the proposed rule as a result of the assertions made by the petitioner in PRM-73-18.

Emergency Preparedness and Safeguards Functions

In the proposed rule for cyber security at FCFs, the NRC staff identifies three specific types of functions (i.e., safety, security, and safeguards) performed by digital assets at fuel cycle facilities that may cause a defined consequence of concern if compromised and therefore potentially require protection from cyber-attacks. The exclusion of emergency preparedness (EP) functions from the FCF cyber security proposed rule and the inclusion of safeguards functions are key differences between the power reactor cyber security rule and the requirements proposed for FCFs.

The final regulatory basis for the “Rulemaking for Cyber Security at Fuel Cycle Facilities” (ADAMS Accession No. ML15355A466) recognized the presence of diverse functions and capabilities such that non-digital redundancies exist for most EP functions at FCFs. Therefore, unlike a power reactor, it is unlikely that a compromise of a digital asset could prevent an FCF licensee from accomplishing the intended EP function (i.e., maintain on-site and off-site communications during normal and emergency operations). The proposed rule for cyber security at FCFs reflects the recommendation in the associated final regulatory basis to require protection of EP functions only in cases where they support (i.e., provide an input to) safety, security, or safeguards functions associated with a consequence of concern.

Unlike power reactors, Category I and II FCFs are required to implement and maintain a material control and accounting system (i.e., safeguards) in accordance with 10 CFR Part 74, “Material Control and Accounting of SNM.” The physical protection and safeguards programs work together to create an integrated and complementary security approach that results in robust protection against sabotage, theft, and diversion of licensed materials. Some FCF licensees currently rely upon digital assets as part of their physical protection and safeguards programs, and other FCF licensees may do so in the future.

The NRC staff does not recommend any changes to the proposed rule’s treatment of EP and safeguards functions as a result of the assertions made by the petitioner in PRM-73-18.

Cyber security and physical protection

A physical protection system is required for controlled access areas at FCFs, pursuant to various NRC security requirements (e.g., 10 CFR 73.20 for Category I FCF licensees, 10 CFR 73.67(a) for Category II and III FCF licensees, and security orders issued to conversion or deconversion licensees). All FCFs are required to have the capability to detect, protect against, and respond to a physical attack. Most digital assets performing safety functions are inherently protected from external physical threats, at a minimum, because access to those assets is limited given their location within the controlled access area; however, there are no physical security requirements specific to the protection of digital assets performing safety functions at FCFs.

The NRC staff does not recommend any changes to the proposed rule's treatment of physical protection functions as a result of the assertions made by the petitioner in PRM-73-18.

Discussion of the Applicability of Petitioner's PRM-73-18 Assertion C to SECY-17-009

Petitioner's Assertion C states that the language in 10 CFR 73.54(a)(1) unnecessarily requires power reactor licensees to focus on protecting hundreds to thousands of digital assets that have no nexus to radiological sabotage. As a result, the considerable time, resources, and costs needed to protect these assets are not justified.

The FCF cyber security proposed rule adopts a graded, consequence-based approach to the protection of digital assets at FCF facilities. It only requires licensees to protect those digital assets that if compromised could result in a defined consequence of concern. The thresholds for determining these consequences of concern have been appropriately tailored to the specific characteristics and licensing basis for each type of FCF facility, including taking into account the appropriate risk and threats associated with each type of facility. The NRC staff has determined that this tailored focus on protecting only those digital assets that can result in a defined consequence of concern will not result in an unnecessary burden on licensees implementing the FCF cyber security rule. The NRC staff recognizes that there will be some burden imposed on licensees by the rule. However, the NRC staff has determined that this burden can be appropriately justified through the corresponding backfit and regulatory analyses developed to support the rule.

The proposed rule avoids a stand-alone focus on cyber security by allowing licensees to take credit for an alternate means of preventing a consequence of concern through the integration of cyber security requirements with the physical security measures currently employed at FCFs. An alternate means of protection would prevent a consequence of concern even if a digital asset is compromised by providing a credible and effective substitute for the function performed by that digital asset. An alternate means of protection could be another digital asset that is protected from a cyber-attack, or an existing feature (e.g., on-site personnel or a physical barrier) that provides an equivalent substitute capable of performing the needed safety, security, or safeguards function in the event of a cyber-attack. If an alternate means of protection is identified for a digital asset, then the proposed rule would not consider that digital asset as vital and no cyber security controls would be required.

The NRC staff does not recommend any changes to the graded, consequence-based approach to the protection of digital assets in the proposed rule as a result of the assertions made by the petitioner in PRM-73-18.

Discussion of the Applicability of Petitioner's PRM 73-18 Assertion D to SECY-17-009

Petitioner's Assertion D states that the Commission's policy decision to apply the NRC's cyber security regulations to structures, systems of components in a nuclear power plant's Balance of Plant (BOP) expanded the scope of 10 CFR 73.54(a) to include digital assets not strictly necessary to be protected to prevent radiological sabotage. While this argument is not directly relevant to FCFs since they do not have a BOP, SECY-17-0099 does contain a potential policy decision relating to the protection of on-site personnel that could uniquely impact and expand the scope of cyber security requirements for FCFs. The NRC staff determined that it was appropriate to discuss petitioner's Assertion D since it raises similar issues relating to the scope of NRC cyber security requirements at nuclear power plants.

The safety consequences of concern defined in the proposed rule for cyber security at FCFs include events that may only impact on-site personnel (i.e., workers). This is a departure from other security rulemakings in that there are not usually requirements to specifically protect on-site personnel from the consequences of a security threat. During the development of the safety consequences of concern defined in the proposed rule, the NRC staff considered several options regarding potential consequence thresholds. Specifically, the staff considered thresholds to require protection against a cyber-attack resulting in: (1) only off-site safety (i.e., radiological and chemical) consequences; (2) off-site safety consequences and on-site radiological consequences; or (3) off-site safety consequences, on-site radiological consequences, and on-site chemical consequences. For the reasons discussed below, the staff determined that option (3) was consistent with the existing licensing basis for FCFs.

The inclusion of a threshold for on-site radiological consequences in the proposed rule addresses cyber-attacks capable of causing an inadvertent criticality, which would be a significant on-site event but may have no off-site impacts. By also including thresholds for on-site chemical consequences (e.g., an acute chemical exposure to a single worker that could lead to irreversible or other serious, long-lasting health effects) in the proposed rule, the identification of digital assets remains consistent with the existing performance requirements in 10 CFR 70.61. The respective licensing bases reflect that the potential for these on-site safety consequences (i.e., inadvertent criticality and acute chemical exposure) is significantly higher for FCF licensees than it is for other NRC licensees (e.g., power reactors). The cyber security requirements for power reactors inherently provide some protection for on-site personnel as most events at a power reactor that would cause on-site consequences would also result in the off-site consequences which power reactor licensees are already required to protect against. The movement of irradiated fuel at a power reactor is an example of a safety-related function that is required to have cyber security protection even though it has the potential for mostly on-site consequences.

The protection of on-site personnel would also limit the potential impact of a cyber-attack used as a coordinated element of a physical attack at an FCF. On-site personnel are often relied upon to provide a mitigative response to safety or security events. A cyber-attack causing an on-site safety consequence of concern could delay, distract, or incapacitate that response. The proposed requirements in SECY-17-0099 allow for the identification of alternate means of protection (i.e., a credible and effective substitute for a function performed by a digital asset that prevents a consequence of concern in lieu of providing cyber security controls). Given the protection that the proposed rule would provide from a cyber-attack capable of causing on-site chemical and radiological exposures, and the lower risk at Category III FCFs and uranium

conversion or deconversion facilities, the NRC staff determined that the applicable physical security staffing requirements at these facilities would be generically acceptable as an alternate means of protection in lieu of requiring additional cyber security for physical protection systems at those FCFs. Accordingly, the proposed rule has no cyber security requirements for physical protection systems at Category III FCFs and uranium conversion or deconversion facilities.

Furthermore, the protection of on-site personnel through the safety consequences of concern in SECY-17-0099 is consistent with DHS CFATS in 6 CFR Part 27, which establish minimum quantities of chemicals as a threshold for applicability of facility-wide protection requirements, including cyber security. Facilities subject to regulation by the NRC are given a statutory exemption by DHS for facilities where NRC already imposes significant requirements and regulates the safety and security of most of the facility. In the overall approach CFATS Appendix A, "DHS Chemicals of Interest," as discussed in 72 FR 65396; November 20, 2007, a facility must establish protections for chemicals of interest where malevolent acts could create a toxicity, flammability, or explosion hazard that would "affect populations within and beyond a facility." DHS also requires site-wide cyber security, which is more burdensome than what is proposed in SECY-17-0099. Although FCF licensees are exempt from DHS's CFATS requirements, the protection of on-site personnel by the NRC's proposed rule for cyber security at FCFs is consistent with overall approach of DHS's requirements for similar chemical facilities.

The Draft Backfit Analysis for SECY-17-0099 provides further evaluation regarding the inclusion of on-site and chemical consequences. The NRC staff does not recommend any changes to the scope of the provisions of the proposed rule pertaining to on-site or chemical consequences as a result of the assertions made by the petitioner in PRM-73-18.

Discussion of the use of a Potential Two-step Cyber Security Plan as part of the NRC's FCF Cyber Security Rule

Through informal engagements with industry stakeholders, the NRC staff has identified a potential enhancement to SECY-17-0099 that could reduce the regulatory burden associated with the FCF cyber security rule. The FCF cyber security proposed rule would currently require, in part, that each FCF licensee submit for NRC review and approval a cyber security plan that describes how the licensee will implement and manage its cyber security program. This cyber security plan must include a discussion of how the licensee would develop and utilize a cyber security team; a configuration management system; identify vital digital assets; establish cyber security controls; protect vital digital assets; provide for event response; and perform event reporting. As written, the proposed rule would require that the cyber security plan satisfy all of these proposed requirements prior to Commission review and approval of the plan.

It is possible that a licensee may discover that they have no vital digital assets at a particular FCF. Through informal engagements with industry stakeholders, licensees have indicated that there may not be a need to develop a full cyber security plan that meets all of the cyber security plan requirements for facilities that have no vital digital assets. Not having to develop a full cyber security plan may reduce licensee costs associated with the rule. Under a two-step cyber security plan, step 1 could require all FCF licensees to provide a cyber security team, utilize a configuration management system, and identify vital digital assets. Step 2 could require the imposition of appropriate security controls on only those digital assets that are determined to be vital because their compromise would result in a defined consequence of concern. This two-step process would likely reduce the burden on licensees resulting from the imposition of controls on digital assets that are not considered vital while maintaining regulatory effectiveness.

The NRC staff is not recommending a change to the FCF cyber security proposed rule. However, staff has determined that there may be value from obtaining stakeholder comment on this proposal during the public comment period on the FCF cyber security proposed rule. Therefore, upon Commission approval of the FCF cyber security proposed rule, the NRC staff plans to conduct public meetings during the public comment period to solicit feedback, ensure a shared understanding of the proposed requirements, and discuss an acceptable approach to implementing the rule's provisions as described in the draft regulatory guide (DG-5062), "Cyber Security Programs for Nuclear Fuel Cycle Facilities" (ADAMS Accession No. ML16319A320). At these public meetings, the NRC staff expects to receive public comments on incorporating the concept of a two-step cyber security plan into the NRC's FCF cyber security final rule. Should the NRC staff determine that implementing a two-step cyber security plan would be beneficial, it would consider proposing a change to the final rule and evaluate whether such a change would constitute a logical outgrowth of the FCF cyber security proposed rule based on comments received.

NRC Staff Conclusion

The NRC staff has determined that there is no reason to modify the scope of the proposed rule for cyber security at FCFs as a result of issues raised in PRM-73-18. The proposed rule for cyber security at FCFs is properly scoped and is justified by the information provided in SECY-17-0099 (i.e., *Federal Register* notice, Draft Backfit Analysis, Draft Regulatory Analysis, and Draft Environmental Assessment). Furthermore, the associated differences between the proposed regulatory requirements for FCFs and the existing requirements for power reactors are adequately justified.