POLICY ISSUE
(Notation Vote)

October 4, 2017 SECY-17-0099

FOR: The Commissioners

FROM: Victor M. McCree
Executive Director for Operations

SUBJECT: PROPOSED RULE – CYBER SECURITY AT FUEL CYCLE FACILITIES (RIN 3150-AJ64; NRC-2015-0179)

PURPOSE:

The purpose of this paper is to obtain Commission approval to publish for public comment a proposed rule to amend Title 10 of the *Code of Federal Regulations* (10 CFR) Part 73, "Physical Protection of Plants and Materials," to establish cyber security requirements for certain nuclear fuel cycle facility (FCF) applicants and licensees.

SUMMARY:

In the March 24, 2015, staff requirements memorandum (SRM) for SECY-14-0147, "Cyber Security for Fuel Cycle Facilities" (Agencywide Documents Access and Management System (ADAMS) Accession No. ML15083A175), the Commission directed the U.S. Nuclear Regulatory Commission (NRC) staff to proceed with a high-priority cyber security rulemaking for FCFs. In response to the Commission's direction, the staff prepared the attached proposed rule that, if approved by the Commission, would amend the current regulations in 10 CFR Part 73, and make conforming changes to additional regulations in 10 CFR Part 40, "Domestic Licensing of Source Material," and Part 70, "Domestic Licensing of Special Nuclear Material," to establish cyber security requirements for certain FCF applicants and licensees. The proposed regulation, if approved, would require FCF applicants and licensees within the scope of the rule to

CONTACTS: Cardelia Maupin, NMSS/MSTR
(301) 415-2312

James Downs, NMSS/FSCE
(301) 415-7744

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. As such, the licensee's cyber security program would enable the licensee to detect, protect against, and respond to a cyber attack capable of causing one or more of the consequences of concern defined in the proposed rule.

As discussed in greater detail below, the proposed requirements would apply to each applicant or licensee subject to the requirements of 10 CFR 70.60, "Applicability," and to each applicant or licensee subject to the requirements of 10 CFR Part 40 for the operation of a uranium hexafluoride conversion or deconversion facility (hereafter FCF licensees).

BACKGROUND:

In SRM-SECY-14-0147, the Commission directed the NRC staff to initiate a high-priority cyber security rulemaking for FCFs and to complete and implement the final rule in an expeditious manner. The Commission also directed the staff to augment the work already performed to develop the technical basis for a proposed rulemaking and to interact with stakeholders in developing the proposed and final rule. Additionally, the Commission directed that in developing its technical basis, the staff should ensure an adequate, integrated look at cyber security as only one aspect of site security (for example, site access controls may provide an element of digital asset protection) and take the requisite care to avoid unintended adverse consequences to safety based on a stand-alone focus on cyber security. Furthermore, the Commission stated that the technical basis should address the need to integrate safety and security and also apply a disciplined, graded approach to the identification of digital assets and a graded, consequence-based approach to their protection. The staff was also directed to monitor licensee implementation of any voluntary cyber security measures undertaken at FCFs during the rulemaking process. Finally, the Commission stated that the staff should consider an 18-month implementation period for the final rule.

Consistent with SRM-SECY-14-0147, and in accordance with the NRC's commitment to openness in its regulatory decision-making, the NRC staff conducted extensive and substantive stakeholder interactions throughout the development of the draft proposed rule, supporting analyses, and associated guidance document. The staff shared relevant documents for public review, conducted site visits, and held 12 public meetings during the period of June 11, 2015, through June 14, 2017.

Between June and July 2015, the NRC staff held two public meetings (ADAMS Accession Nos. ML15174A130 and ML15208A450) to discuss the Commission's direction in SRM-SECY-14-0147, the rulemaking timeline, the proposed graded, consequence-based approach for the rule, licensees' voluntary cyber security efforts, the staff's proposed site visits to learn more about cyber security programs at FCFs, and the status of the FCF cyber security rulemaking draft regulatory basis document.

On September 4, 2015, the NRC staff announced the availability of the draft regulatory basis for public comment in the *Federal Register* (80 FR 53478, ADAMS Accession No. ML15198A024). On September 23, 2015, the staff held a third public meeting (ADAMS Accession No. ML15306A267) during the 30-day comment period to receive stakeholder feedback on the draft regulatory basis.

During the period August 25, 2015, through October 8, 2015, the NRC staff conducted a number of site visits at FCF licensees, including: Honeywell International, Inc. (Metropolis, Illinois); Westinghouse Electric Company (Columbia, South Carolina); Global Nuclear Fuel – Americas (Wilmington, North Carolina); and BWXT Nuclear Operations Group, Inc. (Lynchburg, Virginia). The objective of these site visits was to inform the proposed rulemaking by monitoring licensee implementation of voluntary cyber security measures undertaken at FCFs, as directed by the Commission in SRM-SECY-14-0147. The staff used the information gained from the site visits in the development of the final regulatory basis document (ADAMS Accession No. ML15355A466).

After performing the site visits and considering the public comments on the draft regulatory basis, the NRC staff began development of the final regulatory basis for the FCF cyber security rulemaking. The staff held additional public meetings on October 22, 2015; December 10, 2015; February 18, 2016; and March 17, 2016 (ADAMS Accession Nos. ML15288A514, ML15356A357, ML16054A160, and ML16092A124). The staff used these meetings to obtain additional input from stakeholders on technical issues relating to the development of the final regulatory basis. During these meetings, discussion topics included: the NRC's proposed consequences of concern[1] related to safety, security, and safeguards functions; the NRC's proposed methodology for screening digital assets; cyber security control sets; support systems within the scope of the rule; methods for identifying digital assets; a proposed timeline for conducting periodic reviews of cyber security implementation; lessons learned from the power reactor cyber security rulemaking; and the resolution of public comments on the draft regulatory basis. The staff completed the final regulatory basis on March 24, 2016. On April 12, 2016, the staff announced the availability of the final regulatory basis in the *Federal Register* (81 FR 21449).

After completion of the final regulatory basis, the NRC staff began development of the proposed rule. On May 19, 2016, the staff held its eighth public meeting (ADAMS Accession No. ML16155A442). This meeting provided stakeholders with an opportunity to review and comment on preliminary draft proposed rule language. On August 25, 2016, the staff held its ninth public meeting (ADAMS Accession No. ML16271A019). This meeting provided stakeholders with an opportunity to discuss the revised preliminary draft proposed rule language along with the associated preliminary draft guidance document. On October 12, 2016, the staff held its tenth public meeting (ADAMS Accession No. ML16306A050). This meeting provided stakeholders with an opportunity to discuss projected costs associated with the implementation of the proposed rule. On March 29, 2017, the staff held its eleventh public meeting (ADAMS Accession No. ML17100A111). In addition, the staff continued to make stakeholders aware of the rulemaking as a part of the NRC's 11th Fuel Cycle Information Exchange (FCIX) on June 14, 2017. During the "Cyber Security Roadmap" presentation at the FCIX, the staff discussed the proposed rule and its status.

DISCUSSION:

The NRC staff has developed a proposed rule that would, if adopted, require FCF applicants or licensees subject to 10 CFR 70.60, or subject to 10 CFR Part 40 for operation of a uranium hexafluoride conversion or deconversion facility, to establish, implement, and maintain a cyber

[1] The consequences of concern defined in the proposed rule include the compromise of a digital asset needed to prevent: theft and diversion of special nuclear material (SNM), radiological sabotage, loss of specific material control and accounting functions, loss or unauthorized disclosure of classified information or matter, or certain radiological or chemical exposures.

security program. Accordingly, the proposed requirements would apply to each applicant or licensee that is or plans to be authorized to: (1) possess greater than a critical mass of 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.

The proposed rule would apply a graded, consequence-based approach to the protection of digital assets that takes into account hazards specific to the different types of FCF licensees, namely: (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 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 (Category I, II, III FCFs and uranium conversion or deconversion facilities).

Key Features of the Proposed Rule

The proposed regulation, if approved, would require FCF licensees within the scope of the rule to establish, implement, and maintain a cyber security program to detect, protect against, and respond to a cyber attack capable of causing one or more defined consequences of concern. To meet these cyber security program performance objectives, FCF licensees would be required to: (1) establish and maintain a cyber security team that is structured, staffed, trained, qualified, and equipped to implement the cyber security program; (2) develop a site-specific cyber security plan that the licensee must submit to the NRC for review and approval; (3) identify digital assets that if compromised by a cyber attack, would result in a consequence of concern; (4) determine which of those assets are vital digital assets (VDAs) that require protection;[2] (5) identify and apply cyber security controls for VDAs; (6) provide temporary compensatory measures to meet the cyber security program performance objectives when the cyber security controls are degraded; (7) establish and maintain a configuration management system to ensure that changes to the facility are evaluated prior to implementation; (8) periodically review the cyber security program; and (9) report and track certain cyber security events. The enclosed *Federal Register* notice (Enclosure 1) discusses each of these actions in greater detail.

Digital assets are integrated into various safety, security, and safeguards systems or programs at FCFs. These licensees rely upon these assets for the performance of important safety, security, and safeguards functions. There is currently no regulatory requirement for FCF licensees to perform an analysis to determine if a cyber attack is capable of causing a consequence of concern by compromising these functions. In the proposed rule, the NRC staff identified the three specific types of functions (safety, security, and safeguards) involving digital assets that would require protection from cyber attacks capable of causing a defined

[2] VDAs are those digital assets that if compromised by a cyber attack, would result in a consequence of concern for which no alternate means of preventing the consequence of concern exists. An alternate means could be another digital asset already protected from a cyber attack, or an existing feature (e.g., guard force, physical barrier) that provides an equivalent substitute capable of performing the needed safety, security, or safeguards function in the event of a cyber attack.

consequence of concern. These functions correlate to the types of consequences of concern that the proposed rule would require FCF licensees to protect against through their cyber security programs. The proposed thresholds for the consequences of concern were informed by existing regulatory requirements in 10 CFR Part 70 for safety; Parts 73 and 95, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data," for security; and Part 74, "Material Control and Accounting of Special Nuclear Material," for safeguards. The focus on consequences of concern corresponding to existing safety, security, and safeguards analyses would limit the scope of digital assets covered by the proposed rule and therefore reduce the burden of the rule on FCF licensees. The various consequences of concern defined in the proposed rule are identified and discussed in Section IV of the enclosed *Federal Register* notice.

The "Draft Backfit Analysis and Documented Evaluation for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR 73.53)" (Enclosure 2), presents the NRC staff's evaluation of the proposed cyber security rule with respect to the backfitting provisions in 10 CFR 70.76, "Backfitting." The draft backfit analysis examines the impacts of the proposed rule relative to the current regulatory framework, including existing regulations and orders. Based on this analysis, the staff determined that the proposed rule would constitute a backfit. This backfit is justified, in part, based on the adequate protection exception to the backfit analysis requirement, and, in part, based on a cost-justified substantial increase in overall protection of public health and safety. The adequate protection exception applies to those provisions of the proposed rule associated with: (1) protecting against the design basis threats (DBTs); or (2) the loss or unauthorized disclosure of classified information or matter (10 CFR Part 95, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data"). These provisions of the proposed rule correspond to the security and safeguards consequences of concern. The cost-justified portion of the proposed rule applies to the safety consequences of concern, as discussed in Section V of the enclosed draft backfit analysis.

The proposed rule adopts a graded, consequence-based approach to the protection of digital assets. Consistent with this approach, the scope of the cyber security controls applicable to a specific digital asset is dependent upon the potential consequence that could result from the compromise of that asset. For example, the consequence of concern involving theft or diversion of formula quantities of SSNM (i.e., applicable to Category I FCF licensees) would require more protection, and therefore a more comprehensive set of controls, than the consequence of concern involving unauthorized removal of SNM of moderate strategic significance (i.e., applicable to Category II FCF licensees).

The proposed rule's graded, consequence-based approach to the protection of digital assets limits the burden on FCF licensees by allowing them to focus their cyber security efforts on protecting against only those cyber threats that could compromise VDAs and result in a defined consequence of concern. This approach reduces the number of digital assets at FCFs that licensees are required to protect. The proposed rule also 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.

The proposed rule would also require FCF licensees within the scope of the rule to provide a cyber security plan that accounts for site-specific conditions and describes how the licensee will meet the program performance objectives of the rule. The cyber security plan would be submitted to the NRC for review and approval. The NRC staff has also developed draft regulatory guide (DG-5062), "Cyber Security Programs for Nuclear Fuel Cycle Facilities,"

(ADAMS Accession No. ML16319A320) that provides an acceptable method for establishing, implementing, and maintaining a cyber security program at FCFs subject to the proposed rule. Also provided in DG-5062 are: (1) a template for developing a cyber security plan; (2) an example of a methodology for identifying and evaluating digital assets; and (3) cyber security controls that a licensee may use to protect VDAs. The draft regulatory guide and proposed rule will be available for public comment at the same time.

Implementation of the Proposed Rule

As directed by the Commission in SRM-SECY-14-0147, the NRC staff is considering an 18-month (540-day) implementation period once the rule becomes effective. Within 180 days of publication of the final rule, each FCF licensee would be required to submit, through an application for amendment of its license, a cyber security plan that satisfies the requirements of the new 10 CFR 73.53, "Requirements for cyber security at nuclear fuel cycle facilities." In addition, each FCF applicant who has submitted an application for a license to the Commission prior to the effective date of the final rule would be required to amend its application to include a cyber security plan that satisfies the requirements of the proposed rule. The NRC would review the license amendment request and the associated cyber security plan. If the applicable requirements are met, the license amendment would be granted with specific implementation dates for the cyber security plan specified in the NRC's written approval. As discussed in the enclosed *Federal Register* notice, the staff is considering the following phased implementation schedule: (1) within 180 days of NRC approval of the cyber security plan, each FCF licensee would identify and document VDAs; and (2) within 540 days of NRC approval of the cyber security plan, each FCF licensee would fully implement the approved cyber security plan.

Coordination with the Advisory Committee on Reactor Safeguards

On November 2, 2016, the NRC staff briefed the Advisory Committee on Reactor Safeguards (ACRS), Digital Instrumentation and Control subcommittee (DI&C SC) (ADAMS Accession No. ML16326A417). The staff provided a second briefing to the ACRS, DI&C SC on February 23, 2017 (ADAMS Accession No. ML17107A332). The staff briefed the full ACRS on June 8, 2017 (ADAMS Accession No. ML17195A279). In a letter dated June 9, 2017 (ADAMS Accession No. ML17166A153), the Nuclear Energy Institute (NEI) submitted comments to the ACRS regarding the meeting on June 8, 2017. The staff revised the rulemaking documents, as appropriate, after considering the input provided by the ACRS during the meetings referenced above.

In a memorandum dated June 21, 2017 (ADAMS Accession No. ML17171A209), the ACRS provided the following two recommendations on the proposed rule and the associated guidance document:

1. The proposed rulemaking, draft regulatory guide, and related documents should be issued for public comment.
2. The guidance should be more specific on methods to screen components based on high-level principles as an alternative to a detailed examination of every digital asset. This

approach should be discussed with industry during the public comment period and addressed when the final rule and regulatory guide are completed.

In a letter dated August 31, 2017 (ADAMS Accession No. ML17180A072), the NRC staff provided a formal response to the ACRS recommendations.

Committee to Review Generic Requirements Interactions on the Draft Proposed Rule:

In a memorandum dated May 24, 2017 (ADAMS Accession No. ML17131A355), the Director of the Office of Nuclear Material Safety and Safeguards requested that the Committee to Review Generic Requirements (CRGR) review and endorse the proposed rule package and associated draft regulatory guide for cyber security at FCFs. On June 27, 2017, and July 12, 2017, the NRC staff briefed the CRGR on the proposed rule package. The staff revised the rulemaking documents, as appropriate, after considering the input provided by the CRGR during the meetings referenced above.

In a memorandum dated August 2, 2017 (ADAMS Accession No. ML17200A101), the CRGR endorsed the proposed rule and draft regulatory guide for formal public comment and noted that the rulemaking package, backfit analysis, and guidance document were comprehensive and thorough. The CRGR members indicated that the staff's graded approach and rationale supported thoughtful decision-making and would facilitate development of the final rule. The CRGR also provided the following two comments:

1. Maintain focus on ensuring and communicating that the cost justifications are based on the quantitative assessments that were performed as opposed to qualitative factors.
2. Provide appropriate clarification of the regulatory bases for FCFs licensed under Part 40 since they are not subject to backfitting protections.

To address the CRGR comments, the NRC staff made changes to both the draft backfit analysis (Enclosure 2) and draft regulatory analysis, "Draft Regulatory Analysis for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR 73.53)" (Enclosure 3). To address the first CRGR comment, the draft backfit analysis was clarified to more clearly communicate that quantitative factors are the basis for the cost justified substantial increase in overall protection. To address the second CRGR comment, both the draft backfit and regulatory analyses were revised to discuss the specific sections of the Atomic Energy Act of 1954, as amended, that provide the NRC with the authority to conduct this rulemaking.

Outcome of This Proposed Rule: Advancing the U.S. Nuclear Regulatory Commission's Strategic Goals and Objectives

The proposed rule is consistent with the agency's goals of ensuring adequate protection of public health and safety, and promoting the common defense and security as the risk and complexity of cyber attacks continue to grow. Furthermore, the proposed rule promotes clarity, effectiveness, and openness in the regulatory process by providing an open and transparent regulatory framework that FCF licensees can consistently implement. The provisions of the proposed rule were carefully considered by the staff to ensure that the cyber security requirements would not inhibit a licensee's ability to meet other regulatory requirements. In the area of organizational excellence, the proposed rule supports the openness objective. The rulemaking has been and continues to be conducted in an open and collaborative process. The

staff conducted 12 public meetings to better inform this proposed rule. In addition, the proposed rule and associated draft regulatory guide would be available for public comment for 90 days.

Stakeholder Interactions

As discussed in the background section of this paper, the NRC staff conducted extensive and substantive interactions with stakeholders throughout the development of the draft regulatory basis, final regulatory basis, draft proposed rule, and draft regulatory guide. The staff shared documents for public review, conducted site visits, and held 12 public meetings during the period of June 11, 2015, through June 14, 2017. The staff used these interactions to discuss the topics set forth in the background section above as well as the preliminary proposed rule language, the associated draft regulatory guide, and the projected costs associated with the implementation of the proposed rule. During the 12 public meetings, the staff received limited feedback from non-industry stakeholders, primarily two non-governmental organizations (NGOs). NGO feedback focused on technical clarifications regarding the draft regulatory basis and the proposed rule language. The NGOs generally supported the NRC's initiation of a cyber security rulemaking for FCFs. All of the noted interactions with various stakeholders assisted the staff in developing the technical and cost basis for the proposed rule. Should the Commission approve publication of the proposed rule, the staff would expect additional and perhaps extensive comments from stakeholders during the public comment period.

The NRC staff also received feedback from industry stakeholders. One significant issue raised by industry stakeholders was the applicability of the rule to computer networks accredited by other Federal agencies. The proposed rule does not apply to classified computer systems at FCFs accredited by other Federal agencies. The staff has determined that those existing accreditation processes adequately address cyber threats to classified systems at FCFs. Stakeholders commented that unclassified computer systems at FCFs accredited by other Federal agencies should also be outside the scope of the proposed rule. Based on these comments, the staff initiated dialogue with the three Federal entities (i.e., National Nuclear Security Administration, Naval Reactors, and the U.S. Department of Energy's Oak Ridge Office) involved with the accreditation of unclassified systems at FCFs. The staff will assess the protection provided to digital assets residing on these unclassified systems after the respective Federal entities finalize revisions to their requirements for accreditation. A final decision on this issue will not be made until this assessment is completed.

Following the public meeting on October 12, 2016, NEI submitted a letter to the NRC staff dated October 19, 2016 (ADAMS Accession No. ML16315A290), expressing concerns about the proposed rule. One of NEI's principal concerns was that the rule would impose cyber security requirements on FCF licensees that are not currently subject to the DBTs. NEI is correct that the proposed rule would affect FCF licensees not subject to the DBTs, as currently only Category I FCF licensees are subject to the DBTs. However, the Interim Compensatory Measure Orders issued between 2002 and 2003 require FCF licensees, including those not subject to the DBTs (i.e., Category III FCF licensees), to protect against cyber threats. Since then, the cyber threat has continued to evolve and FCF licensees have become more dependent on digital technology to implement safety, security, and safeguards functions. As discussed above and in the draft regulatory analysis, the proposed rule would apply a graded, consequence-based approach to protecting digital assets whose compromise by a cyber attack would result in one or more consequences of concern at those FCFs within the scope of the proposed rule, including Category I and III FCF licensees.

In its letter, NEI also expressed a concern that the proposed rule should reflect the outcome of the petition review process for its previously submitted petition for rulemaking (PRM)-73-18, "Protection of Digital Computer and Communication Systems and Networks." In its PRM, NEI requested that the NRC revise its power reactor cyber security regulations by narrowing the scope of 10 CFR 73.54, "Protection of digital computer and communication systems and networks," to those structures, systems, and components that are either necessary to prevent core damage and spent fuel sabotage, or whose failure would cause a reactor scram. The NRC staff is currently evaluating the PRM. The staff recognizes that, depending on the outcome of the petition review process as it relates to the DBT, PRM-73-18 may have the potential to impact the scope of this rulemaking. If the NRC accepts the PRM and narrows the scope of the safety and security functions protected by the provisions of 10 CFR 73.54, the NRC staff would have to determine if this change in the power reactor rule would impact the scope of safety and security functions considered in the proposed FCF cyber security rule. As noted in SECY-14-0147, "Cyber Security for Fuel Cycle Facilities" (not publicly available because it contains security-related information), the staff will consider how the resolution of the subject PRM affects this rulemaking to the extent that it is relevant to FCF licensees. Once the decision on PRM-73-18 is made, the staff will determine if any corresponding changes are necessary.

Finally, NEI's letter described other concerns related to industry cost estimates for implementation of the proposed rule, development of the cyber security plan, and staffing a cyber security team. Additionally, NEI raised concerns regarding the burden of screening digital assets, documenting VDAs, and the possible exclusion of digital assets that are part of an unclassified system accredited by another Federal agency. As a result of NEI's feedback, the NRC staff revised the cost estimates and incorporated the associated insight gained from the discussions with NEI into the enclosed draft regulatory analysis. Based on comments received from stakeholders, the staff modified the draft regulatory guide to include an acceptable method for screening digital assets and documenting VDAs that minimizes burden on licensees.

Implementing Guidance

The NRC staff has developed DG-5062 (ADAMS Accession No. ML16319A320) to assist licensees in the implementation of the proposed rule. The draft regulatory guide describes a method that the staff considers acceptable for use in complying with the cyber security requirements in the proposed rule. Because the enclosed draft regulatory analysis provides sufficient discussion of both the proposed rule and DG-5062, a separate regulatory analysis was not prepared for the draft regulatory guide. The draft regulatory guide and the proposed rule will be available for public comment at the same time.

Potential Policy Considerations

The following features of the proposed rule have been identified by senior staff management as being worthy of specific mention to the Commission for consideration in its decision-making process.

First, by requiring licensees to protect against a cyber attack capable of causing a compromise of functions needed to prevent the loss or unauthorized disclosure of classified information or classified matter as part of the consequences of concern defined in the proposed rule, the agency is expanding its regulatory scheme for the protection of classified information. The proposed rule addresses an absence of specific cyber security provisions in 10 CFR Part 95 applicable to the protection of classified information or matter at FCFs. However, the NRC also addresses the protection of classified information generally by working with other federal

agencies. In accordance with Executive Order 12829, "National Industrial Security Program," the NRC consults with the U.S. Secretary of Defense and provides its concurrence on the Department of Defense's (DoD's) Operating Manual 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)." The NISPOM provides baseline standards for the protection of classified information for the Federal government and its contractors, grantees, and licensees. The NRC is one of five signature authorities for the NISPOM, and as such, the NRC has a shared responsibility with DoD for the document's content. While currently the standards in the NISPOM do not conflict with the requirements in the proposed rule, the NRC staff needs to remain fully engaged with respect to future proposed NISPOM changes as part of its efforts in working with DoD to avoid overlapping or potentially conflicting requirements with cyber security regulations for FCF licensees. If the staff is not successful in preventing conflicts between the NISPOM and the proposed cyber security rule, inclusion of cyber security provisions specific to the protection of classified information in a cyber security rule could create the potential need for selected exemptions to the rule.

Second, the safety consequences of concern defined in the proposed rule include events that may only impact on-site personnel. This is a departure from other security rulemakings in that there is not usually a requirement 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. While for other types of licensees (e.g., operating reactor licensees) the NRC has typically focused on establishing performance objectives/requirements that are protective of the public rather than on-site personnel, the staff determined that option (3) was more consistent with the existing regulatory approach used for FCF licensees. The inclusion of a threshold for on-site radiological consequences in the proposed rule addresses cyber attacks capable of causing a 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 is tied to the existing performance requirements in 10 CFR 70.61. The benefits and costs of this approach are discussed in the draft regulatory and backfit analyses.

In contrast to the approach taken in the proposed rule, other regulatory frameworks, such as the Department of Homeland Security's Chemical Facility Anti-Terrorism Standards (CFATS), establish minimum quantities of chemicals as a threshold for applicability of facility-wide protection requirements. Under CFATS, a facility does not need to establish protections for chemicals of interest in amounts below these minimum quantity thresholds because malevolent acts could not create a toxicity, flammability, or explosion hazard that would "affect populations within and beyond a facility." In essence, the CFATS regulatory framework is consequence-based, however, it is different from the graded, consequence-based approach used in the proposed cyber security rule in that the rule defines the consequence threshold (e.g., a radiological exposure of 25 rem or greater for any individual, an 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), whereas the CFATS consequence thresholds are not defined.

Third, the proposed rule does not provide a means for licensees to modify the facility in such a way as to obviate the need for a cyber security program, even if the facility has no vital digital assets. Rather, the program would be required to be in place to provide for configuration management (i.e., the assessment of future changes to the facility). In focusing on the observed conditions at existing FCFs while developing the proposed rule, the NRC staff concluded that all FCF licensees should be required to establish and maintain a cyber security program, including a cyber security plan and team, even if the licensee has no vital digital assets. Under the proposed rule, the cyber security plan would describe the methodology by which a FCF licensee identifies digital assets and determines vital digital assets. The cyber security plan, including the referenced methodology, would be reviewed and approved by the NRC prior to the FCF licensee performing the required analysis of digital assets. This would establish a licensing basis for the NRC's inspection of the FCF licensee's analysis of digital assets. Furthermore, the cyber security plan would also formalize an enforceable commitment by the FCF licensee to utilize a configuration management system, perform a periodic review of cyber security, and report events caused by cyber attacks. The benefits and costs of this approach are discussed in the draft regulatory and backfit analyses.

The staff acknowledges that the approach requiring all FCF licensees to establish and maintain a cyber security program imposes a regulatory burden and that the proposed rule does not provide a means for FCF licensees to avoid having to establish a cyber security program altogether by either designing or redesigning their facilities to incorporate an effective defensive architecture that provides adequate cyber protection. In other words, a licensee may not find it beneficial to modify its facility by introducing a defensive architecture because it would not completely eliminate the burden of maintaining a cyber security program. Although the staff recognizes that an effective defensive architecture would provide adequate cyber security, as stated in the formal response to the ACRS recommendations (ADAMS Accession No. ML17180A072), the staff views configuration management as an important element of maintaining effective cyber security to ensure that future changes do not introduce a vulnerability that could be exploited by a cyber attack causing a consequence of concern. The proposed rule and draft regulatory guide do, however, attempt to minimize regulatory burden, as discussed in the formal response to the ACRS recommendations. Notwithstanding, the staff plans to conduct additional stakeholder interactions during the public comment period that may provide further information on methods to minimize the regulatory burden.

COMMITMENT:

The NRC staff plans to conduct an additional public meeting to facilitate stakeholder comments during the public comment period for the proposed rule and draft regulatory guide.

RESOURCES:

The resources associated with this rulemaking are addressed in Enclosure 5, which is not publicly available.

RECOMMENDATIONS:

That the Commission:

1. Approve for publication, in the *Federal Register*, the proposed rule (Enclosure 1) amending 10 CFR Parts 40, 70, and 73.

2. Note:

   a. The proposed amendments will be published in the *Federal Register*, allowing 90 days for public comment;

   b. The Chief Counsel for Advocacy of the Small Business Administration will be informed of the certification that the rule will not have a significant economic impact on a substantial number of small entities, and the reasons for the certification, as required by the Regulatory Flexibility Act, 5 U.S.C. 605(b);

   c. A draft backfit analysis has been prepared for the proposed rule (Enclosure 2);

   d. A draft regulatory analysis has been prepared for the proposed rule (Enclosure 3);

   e. A draft environmental assessment, "Draft Environmental Assessment and Finding of No Significant Impact for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR 73.53)," has been prepared for the proposed rule (Enclosure 4);

   f. The appropriate Congressional committees will be informed of this action; and

   g. An Office of Management and Budget (OMB) review is required and a clearance package will be forwarded to OMB no later than the date the proposed rule is submitted to the Office of the Federal Register for publication.

COORDINATION:

The Office of the General Counsel has reviewed this paper and has no legal objection. The Office of the Chief Financial Officer has reviewed this paper for resource implications and has no objections.

/RA/

Victor M. McCree
Executive Director
for Operations

Enclosures:
1. *Federal Register* Notice
2. Draft Backfit Analysis
3. Draft Regulatory Analysis
4. Draft Environmental Assessment
5. Resources

SUBJECT: PROPOSED RULE – CYBER SECURITY AT FUEL CYCLE FACILITIES (RIN 3150-AJ64; NRC-2015-0179), DATED: OCTOBER 4, 2017.

DISTRIBUTION:
EDO Control RidsEdoMailCenter RidsNSIRMailCenter

ML17018A218 **SRM-S14-0147-3**

OFC	NMSS/MSTR	NMSS/MSTR	NMSS/MSTR	NMSS/FCSE	NSIR/CSD	OCIO	CFO	OE
NAME	CMaupin	KMorgan-Bulter	DCollins	CErlanger via email	JAndersen via email	DCullison via email	RAllewein; MLee for via email	PHolahan; TMarenchin for via email
DATE	11/18/16 01/25/17	11/22/16	4/27/17	4/26/17	12/06/16	01/26/17	12/21/16	01/12/17
OFC	ADM	NSIR	OGC	Tech Editor	NMSS	EDO		
NAME	CBladey via email	BHolian; SWest for via email	NStAmour via email	WMoore via email	MDapas	VMcCree		
DATE	01/17/2017	12/29/17	04/18/17	04/25/17	9/7/17	10/04/17		

OFFICIAL RECORD COPY