[7590-01-P]

NUCLEAR REGULATORY COMMISSION

10 CFR Parts 40, 70, and 73

[NRC-2015-0179]

RIN 3150-AJ64

Cyber Security at Fuel Cycle Facilities

AGENCY: Nuclear Regulatory Commission.

ACTION: Proposed rule and guidance: request for comment.

SUMMARY: The U.S. Nuclear Regulatory Commission (NRC) is proposing to amend its security regulations for the 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. Concurrently, the NRC is also issuing for public comment a new draft regulatory guide (DG), DG-5062, "Cyber Security Programs for Nuclear Fuel Cycle Facilities," for use in the implementation of the proposed requirements in this rulemaking.

DATES: Submit comments on the proposed rule by **[INSERT DATE THAT IS 90 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**. Submit comments specific to the information collections aspects of the proposed rule by **[INSERT DATE THAT IS 30**

DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. Comments received after these dates will be considered if it is practical to do so, but the NRC is able to ensure consideration only for comments received on or before these dates.

ADDRESSES: You may submit comments by any of the following methods (unless this document describes a different method for submitting comments on a specific subject):

- **Federal Rulemaking Website:** Go to http://www.regulations.gov and search for Docket ID NRC-2015-0179. Address questions about NRC dockets to Carol Gallagher; telephone: 301-415-3463; e-mail: Carol.Gallagher@nrc.gov. For technical questions contact the individual(s) listed in the FOR FURTHER INFORMATION CONTACT section of this document.
- **E-mail comments to:** Rulemaking.Comments@nrc.gov. If you do not receive an automatic e-mail reply confirming receipt, then contact us at 301-415-1677.
- **Fax comments to:** Secretary, U.S. Nuclear Regulatory Commission at 301-415-1101.
- **Mail comments to:** Secretary, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, ATTN: Rulemakings and Adjudications Staff.
- **Hand deliver comments to:** 11555 Rockville Pike, Rockville, Maryland 20852, between 7:30 a.m. and 4:15 p.m. (Eastern Time) Federal workdays; telephone: 301-415-1677.

For additional direction on obtaining information and submitting comments, see "Obtaining Information and Submitting Comments" in the SUPPLEMENTARY INFORMATION section of this document.

FOR FURTHER INFORMATION CONTACT: Cardelia H. Maupin, Office of Nuclear Material Safety and Safeguards (NMSS), telephone: 301-415-2312, email: Cardelia.Maupin@nrc.gov,

U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

SUPPLEMENTARY INFORMATION:

I. Executive Summary

A. Need for the Regulatory Action

The NRC is proposing to amend its regulations related to certain FCF applicants and

licensees. The proposed rule would amend part 73 of title 10 of the *Code of Federal Regulations* (10 CFR), "Physical Protection of Plants and Materials," to require that FCF applicants and licensees establish, implement, and maintain a cyber security program 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. The requirements of the proposed rule, if approved, would apply to each applicant or 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 applicants or licensees subject to 10 CFR 70.60, "Applicability," or subject to 10 CFR part 40, "Domestic Licensing of Source Material," for operation of a uranium hexafluoride conversion or deconversion facility. Hereafter, the FCF applicants and licensees for which the proposed rule would be applicable will be referred to as "FCF licensees."

Each FCF licensee is subject to either the design basis threats (DBTs) set forth in 10 CFR 73.1, "Purpose and scope," or to the Interim Compensatory Measures (ICM) Orders issued to all FCF licensees in 2002 and 2003. Both the DBTs and the ICM Orders contain a requirement that these licensees include consideration of a cyber attack when considering security vulnerabilities. However, the NRC's current physical protection regulations in 10 CFR part 73 do not provide specific requirements or guidance on how to implement these performance objectives. Given the evolution in the cyber threat to FCFs since the ICM Orders were issued and the DBT rule was revised, specific cyber security requirements for FCF licensees are warranted.

B. Major Provisions

Major provisions of the proposed rule include requirements that would:

- Establish and maintain a cyber security program to implement a graded, performance-based regulatory framework for the protection of digital computer systems, communications systems, and networks.
- Identify digital assets associated with safety, security (both physical and information security), and safeguards functions that if compromised by a cyber attack, would result in one or more of the specific consequences of concern defined in the proposed rule.
- Protect vital digital assets (VDAs) by selecting, applying, and maintaining appropriate cyber security controls.[1]
- Apply and maintain defense-in-depth protective strategies to ensure the capability to detect and respond to a cyber attack.
- Maintain configuration management of digital assets that if compromised by a cyber attack, would result a consequence of concern.

C. Benefits and Costs

The NRC prepared "Draft Regulatory Analysis for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR 73.53)" (the NRC's Agencywide Documents Access and Management System (ADAMS) Accession No. ML16320A452), to discuss the expected quantitative benefits and costs of the proposed rule, as well as set forth the qualitative factors

[1] 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.

considered in the NRC's rulemaking decision. The key findings of the draft regulatory analysis, including a table that summarizes the costs by entity, are as follows:

- **Benefits.** The proposed rule would ensure that FCF licensees protect VDAs from a cyber attack capable of causing one or more of the following specific consequences of concern:

1) Significant exposure events that could endanger the life of workers or could lead to irreversible or other serious, long-lasting health effects to workers or members of the public (e.g., nuclear criticalities and releases of radioactive materials or chemicals);

2) Radiological sabotage and theft or diversion of formula quantities of strategic special nuclear material (SSNM);

3) Loss of control and accounting of formula quantities of SSNM;

4) Unauthorized removal of SNM of moderate strategic significance;

5) Loss of control and accounting of SNM of moderate strategic significance; or

6) Loss or unauthorized disclosure of classified information.

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 DBT rule was revised. The NRC staff has observed that cyber attacks have exploited security vulnerabilities at global critical infrastructure facilities, including global FCFs, similar to the potential security vulnerabilities that the 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 defined consequences of concern.

The FCF licensees subject to the ICM orders or the DBTs are required to consider cyber security vulnerabilities in the design of their protective strategies. However, the NRC's regulatory structure does not set forth specific requirements or guidance on how these vulnerabilities should be addressed. For example, there are no regulatory requirements for FCF licensees to analyze, identify, or protect digital assets that if compromised by a cyber attack,

would result in a defined consequence of concern.

The proposed rule adopts a graded, consequence-based approach that would require licensees to identify and protect only those digital assets necessary to prevent a defined consequence of concern. The NRC staff has adopted this approach to reduce the potential burden of the proposed rule on FCF licensees. Additionally, this graded, consequence-based approach would only require licensees to protect against those consequences of concern that are applicable to their facility. The proposed rule would also allow licensees the flexibility to credit existing alternative means of protecting against a consequence of concern that they may already be implementing for other purposes. The staff has determined that the proposed rule sets forth a tailored and efficient approach for protecting against the cyber threat faced by FCF licensees.

The NRC staff has identified numerous benefits that would be provided by the proposed rule, but recognizes that FCF licensees would incur implementation costs. As set forth in Table 1 and in the draft regulatory analysis prepared for the proposed rule, the staff has analyzed potential implementation costs for the various types of FCF licensees. Given the complexity of quantifying the character and likelihood of events due to malicious attacks, the staff was unable to quantify several of the benefits and costs associated with the reduction in risk achieved as a result of mitigating a cyber security threat. Accordingly, the draft regulatory analysis sets forth a qualitative assessment of several of the benefits and costs of the proposed rule. For more information, please see Section 4 of the draft regulatory analysis. Based on this analysis, the staff has determined that the costs associated with implementing the proposed rule are reasonable given the benefits to public health and safety and common defense and security associated with preventing a potential consequence of concern at a FCF. Therefore, the draft regulatory analysis concludes that the proposed rule is cost-justified and should be adopted.

- **Cost to the Industry**. The proposed rule would result in an estimated, average,

undiscounted implementation cost per licensee of approximately $550,000, followed by an estimated, undiscounted, average, annual operational cost of approximately $152,000 over the 25-year regulatory analysis period for each licensee. Overall, the industry (i.e., eight impacted FCF licensees) would incur an estimated, undiscounted implementation total cost of approximately $4,400,000, followed by an estimated, undiscounted, annual operational cost of approximately $1,200,000 over the regulatory analysis period.

- **Cost to the NRC**. The proposed rule would result in an undiscounted implementation cost to the NRC of an estimated $1,900,000, followed by an estimated, undiscounted, average, annual operational cost of $120,000 over the regulatory analysis period.

Table 1 **– Summary of Costs by Entity Over the 25-year Analysis Period**

Entity	One-time Implementation Costs	Recurring and Annual Operating Costs	Total Combined Implementation and Annual Costs Undiscounted	Present Value Combined Implementation and Annual Cost at 3% Discount Rate	Present Value Combined Implementation and Annual Cost at 7% Discount Rate
Industry Costs	($4,364,000)	($1,215,000)	($34,727,000)	($25,513,000)	($18,518,000)
NRC Costs	($1,918,000)	($123,000)	($4,990,000)	($4,058,000)	($3,350,000)
Total	($6,283,000)	($1,337,000)	($39,717,000)	($29,571,000)	($21,868,000)

*Note dollars are rounded to the nearest 1,000th

II. Obtaining Information and Submitting Comments

A. Obtaining Information

Please refer to Docket ID **NRC-2015-0179** when contacting the NRC about the availability of information for this action. You may obtain publicly-available information related to this action by any of the following methods:

- **Federal Rulemaking Web Site:** Go to http://www.regulations.gov and search for Docket ID **NRC-2015-0179**.
- **NRC's Agencywide Documents Access and Management System (ADAMS):** You may obtain publicly-available documents online in the ADAMS Public Documents collection at http://www.nrc.gov/reading-rm/adams.html. To begin the search, select "ADAMS Public Documents" and then select "Begin Web-based ADAMS Search." For problems with ADAMS, please contact the NRC's Public Document Room (PDR) reference staff at 1-800-397-4209, 301-415-4737, or by e-mail to pdr.resource@nrc.gov. The ADAMS accession number for each document referenced in this document (if that document is publically available in ADAMS) is provided the first time that a document is referenced. For the convenience of the reader, the ADAMS accession numbers are provided in the "Availability of Documents" section of this document.
- **NRC's PDR:** You may examine and purchase copies of public documents at the NRC's PDR, Room O1-F21, One White Flint North, 11555 Rockville Pike, Rockville, Maryland 20852.

B. Submitting Comments

Please include Docket ID **NRC-2015-0179** in the subject line of your comment submission, in order to ensure that the NRC is able to make your comment submission available to the public in this docket.

The NRC cautions you not to include identifying or contact information that you do not

want to be publicly disclosed in your comment submission. The NRC will post all comment submissions at http://www.regulations.gov as well as enter the comment submissions into ADAMS. The NRC does not routinely edit comment submissions to remove identifying or contact information.

If you are requesting or aggregating comments from other persons for submission to the NRC, then you should inform those persons not to include identifying or contact information that they do not want to be publicly disclosed in their comment submission. Your request should state that the NRC does not routinely edit comment submissions to remove such information before making the comment submissions available to the public or entering the comment into ADAMS.

III. Background

A. Post-September 11, 2001

After the terrorist attacks of September 11, 2001, the NRC issued a series of security orders to FCF licensees. These orders were referred to as ICM Orders, and addressed the threat environment at that time by imposing additional security requirements beyond those existing in 10 CFR 73.20, “General performance objective and requirements,” 73.40, “Physical protection: General requirements at fixed sites,” 73.45, “Performance capabilities for fixed site physical protection systems,” 73.46, “Fixed site physical protection systems, subsystems, components, and procedures,” and 73.67, “Licensee fixed site and in-transit requirements for the physical protection of special nuclear material of moderate and low strategic significance.” The ICM Orders also directed licensees to evaluate and address cyber security vulnerabilities at their facilities.

Since the issuance of the ICM Orders, the threats to digital computer systems,

communications systems, and networks—hereafter collectively referred to as “digital assets”—have substantially increased both globally and nationally. Cyber attacks have increased in number, become more sophisticated, resulted in physical consequences, and targeted digital assets similar to those in safety, security, and safeguards systems utilized by FCF licensees. Unlike a physical attack on a FCF licensee, a cyber attack can occur remotely, by anonymous individuals, with little fear of discovery or arrest on the part of the attacker.

B. Design Basis Threat Rulemaking

Section 651 of the Energy Policy Act of 2005 (EPAct 2005) directed the NRC to initiate a rulemaking to revise the DBTs set forth in 10 CFR 73.1, “Purpose and scope,” and to consider, at a minimum, 12 factors when developing the DBT rulemaking, including a potential cyber threat. The DBTs are used by 10 CFR part 70, “Domestic Licensing of Special Nuclear Material,” licensees authorized to possess or use a formula quantity of SSNM, as defined in 10 CFR 70.4, “Definitions,” and 73.2, “Definitions” (Category I FCF licensees), to form the basis for site-specific defensive strategies that are based on realistic assessments of the tactics, techniques, and procedures used by terrorist groups, organizations, or individuals. Specifically, DBTs are used by Category I FCF licensees to design safeguards systems to protect against acts of radiological sabotage and to prevent theft or diversion of NRC-licensed SSNM. In response to the EPAct 2005, the NRC published a rule entitled “Design Basis Threat” (72 FR 12705; March 19, 2007), which revised 10 CFR 73.1 to explicitly include a cyber attack as an element of the DBTs.

C. Power Reactor Regulatory Requirements

The NRC addressed the cyber security threat within the applicable radiological sabotage DBT for nuclear power plants with the publication of the final rule, “Power Reactor Security

Requirements" (74 FR 13926; March 27, 2009). The rule included new requirements set forth in 10 CFR 73.54, "Protection of digital computer and communication systems and networks." This new regulation substantially expanded upon the cyber requirements imposed by the ICM Orders for power reactors. It requires power reactors to provide high assurance that digital assets essential for plant safety, security, and emergency preparedness functions are protected from a cyber attack up to and including the DBT for radiological sabotage as established by 10 CFR 73.1(a)(1)(v). The NRC staff used the experience and knowledge gained during the development and implementation of 10 CFR 73.54 to inform its graded, consequence-based approach for developing cyber security requirements for FCF licensees.

D. Fuel Cycle Cyber Security Working Group

In 2010, the NRC formed a FCF cyber security working group (NRC working group) to build upon experiences gained during the development and implementation of the 10 CFR 73.54 cyber security rule for nuclear power reactors. The NRC working group reviewed cyber security measures at FCFs to determine how FCF licensees protect their digital assets from a cyber attack and to determine whether additional regulatory action was needed to strengthen the protection of these digital assets. In conducting its review, the NRC working group consulted existing national cyber security standards, including the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems, Revision (Rev) 1" (NIST SP 800-37, Rev 1, February 2010), and NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations, Rev 4" (NIST SP 800-53, Rev 4, April 2013). These NIST standards informed the NRC staff's evaluation of the cyber security measures implemented by FCF licensees. The NIST standards are generally accepted in the cyber security industry and have been used for developing Federal cyber security programs. These

documents are available online at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf and http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

The referenced NIST publications address a diverse set of security and privacy requirements derived from legislation, Executive Orders, policies, directives, regulations, and standards for both the United States Federal Government and the nation's critical infrastructure. NIST SP 800-37, Rev 1, describes dynamic approaches for improving information security and strengthening risk management processes through the use of a risk management framework. NIST SP 800-53, Rev 4, describes how to develop specialized sets of controls, or overlays, tailored for specific types of functions, technologies, or environments of operation. Also, NIST SP 800-53, Rev 4, catalogs cyber security controls that address both functionality (the strength of cyber security functions and mechanisms provided) and assurance (the measures of confidence achieved from the implemented cyber security capability).

In conducting its reviews of FCF licensees, the NRC working group designed a four-step assessment process that consisted of: 1) requesting FCF licensees to respond to an NRC questionnaire regarding the extent to which digital assets were used for critical functions, such as safety, security, emergency preparedness, and material control and accounting (SSEPMCA); 2) performing site visits and phone interviews with FCF licensees; 3) analyzing licensees' documentation of their cyber security actions and observing how the programs were implemented; and 4) documenting the results of the assessments in a final report. During site visits conducted in 2011, the NRC working group examined a number of digital assets performing, supporting, or associated with SSEPMCA functions. The NRC working group determined that the compromise of these digital assets could result in an impact on public health and safety or common defense and security. Additionally, the NRC working group assessed FCF licensees' voluntary cyber security initiatives. Furthermore, the NRC working

group sought feedback from interested stakeholders during public meetings on the NRC's proposed graded, consequence-based approach to evaluating FCF cyber security.

In February 2012, the NRC working group issued its final report (not publicly available because it contains security-related information). The report discussed the NRC staff's observations from their multiple site visits to FCF licensees and noted that the scope of licensee cyber security actions, policies, and procedures varies greatly across the fuel cycle industry. FCF licensees relied on a variety of digital technologies for the performance of SSEPMCA functions. These technologies ranged from information technology equipment and software to specialized commercial, proprietary, and hybrid industrial automation systems. As a result of the site visits and ongoing interactions with industry stakeholders, the staff determined that additional cyber security requirements were necessary for FCFs.

E. NRC Interactions with Industry Stakeholders on Voluntary Initiatives

Based on the site visits and interactions with stakeholders during public meetings, the NRC working group identified six near-term cyber security measures that, if voluntarily implemented by FCF licensees, would enhance the protection of FCF digital assets from a cyber attack. These measures included: 1) creating a cyber security team; 2) providing cyber security awareness training to FCF staff; 3) developing a capability for incident response to a cyber attack capable of causing a consequence of concern; 4) implementing security controls that address portable media, devices, and equipment; 5) conducting a baseline assessment of digital assets performing SSEPMCA functions to understand the connections between digital assets and other systems, interactions between digital assets, and interdependencies between digital assets; and 6) implementing security controls to isolate digital assets performing critical SSEPMCA functions from external, network based attack vectors.

During meetings with industry stakeholders, the NRC staff encouraged FCF licensees to

propose approaches to voluntarily adopt the above-referenced six near-term measures to protect digital assets at FCFs. The Nuclear Energy Institute (NEI) and FCF licensees responded to the NRC's potential paths forward (i.e., performance of a voluntary initiative by FCF licensees, issuance of security orders, or initiating a rulemaking) in letters dated January 17, 2013; July 3, 2013; and May 19, 2014 (not publicly available because they contain security-related information). The FCF licensees generally indicated that they were willing to implement the first four near-term measures identified by the staff. However, FCF licensees did not agree with implementing the staff's final two near-term measures. Furthermore, the FCF licensees did not agree with the NRC working group's recommendation to incorporate licensee voluntary cyber security measures into a license condition that would be subject to the NRC's regulatory oversight and enforcement.

While the NRC working group continued its work, the NRC staff developed SECY-12-0088, "The Nuclear Regulatory Commission Cyber Security Roadmap," dated June 25, 2012 (ADAMS Accession No. ML12135A050). In SECY-12-0088, the staff set forth its "roadmap" for evaluating the need to enhance cyber security requirements for FCFs, non-power reactors, independent spent fuel storage installations, and byproduct materials licensees. With respect to FCFs, the staff determined that a rulemaking using a graded, consequence-based approach to address cyber security for digital assets at FCFs should be considered. A recent update, provided in SECY-17-0034, "Update to the U.S. Nuclear Regulatory Commission Cyber Security Roadmap," dated February 28, 2017 (ADAMS Accession No. ML16354A258), reflects the progress made by the staff in developing that approach.

The NRC staff also informed the Commission in SECY-12-0088 of the staff's ongoing discussions with NEI and FCF licensees on the six near-term voluntary cyber security measures. The staff stated that if the industry decided not to participate in this voluntary initiative, or if the resulting changes did not generate the desired outcome of strengthening

existing FCF cyber security programs, the NRC would consider the issuance of orders.

F. 2014 NRC Staff Recommendations on Fuel Cycle Cyber Security

In SECY-14-0147, “Cyber Security for Fuel Cycle Facilities,” dated December 30, 2014 (not publicly available because it contains security-related information), the NRC staff summarized the efforts of the NRC working group and provided recommendations to the Commission for addressing cyber security at FCFs. The Commission paper set forth the staff’s determination that the voluntary cyber security measures being pursued by FCF licensees did not fully address the protection of digital assets performing SSEPMCA functions at FCFs. Therefore, additional cyber security requirements were needed to protect against a cyber attack given the persistent and evolving cyber security threat, the potential exploitation of vulnerabilities at FCFs through multiple attack vectors, the inherent difficulty of detecting the compromise of digital assets, and the potential consequences associated with a cyber attack. The staff recommended to the Commission that security orders be issued to FCF licensees requiring them to implement the six near-term voluntary measures identified by the staff, followed by a cyber security rulemaking using a graded, consequence-based approach for cyber security at FCFs.

G. Commission Direction on Fuel Cycle Cyber Security

In the staff requirements memorandum (SRM) for SECY-14-0147, “Cyber Security for Fuel Cycle Facilities,” dated March 24, 2015 (ADAMS Accession No. ML15083A175), the Commission disapproved the NRC staff’s recommendation to issue a security order to FCFs. The Commission directed the 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.

H. Stakeholder Interactions on Rulemaking

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 June 11, 2015, through June 14, 2017.

Stakeholder Interactions on the Draft Regulatory Basis:

Stakeholders provided input throughout the development of the regulatory basis. The NRC staff held two public meetings on June 11, 2015 (ADAMS Accession No. ML15174A130), and on July 13, 2015 (ADAMS Accession No. ML15208A450), to discuss the draft regulatory

basis. On September 4, 2015, the staff announced the availability of the draft regulatory basis for public comment in the *Federal Register* (80 FR 53478). The comment period was for 30 days and closed on October 5, 2015. During the comment period, the staff held a third public meeting on September 23, 2015 (ADAMS Accession No. ML15306A267). In addition to feedback from the meetings, a number of formal comments were provided by FCF licensees and NEI (see the comment resolution document at ADAMS Accession No. ML15355A469).

Cyber Security Site Visits:

During the period August 25 through October 8, 2015, the NRC staff conducted a number of site visits at FCFs including: Honeywell International, Inc. (Metropolis, IL); Westinghouse Electric Company (Columbia, SC); Global Nuclear Fuel – Americas (Wilmington, NC); and BWXT Nuclear Operations Group, Inc. (Lynchburg, VA). The objective of these site visits was to inform the proposed rulemaking by monitoring implementation of voluntary cyber security measures undertaken by FCF licensees. The staff summarized the information gained from the site visits in a report dated January 11, 2016 (ADAMS Accession No. ML15292A098).

During these site visits, the NRC staff observed that all of the FCF licensees were generally proactive in addressing cyber security concerns. The staff observed areas of improvement since the 2011 and 2013 site visits, and noted that all of the FCF licensees had plans for further improvement. However, the staff determined that FCF licensee voluntary cyber security measures lacked a level of rigor commensurate with the evolving cyber threat and the potential for a consequence of concern at FCFs. Licensee voluntary cyber security measures failed to include comprehensive analyses of cyber security vulnerabilities and were not based on a robust risk-management methodology derived from an industry recognized standard such as NIST SP 800-37, Rev 1, or NIST SP 800-54, Rev 4. In addition, licensee voluntary cyber security measures addressed only a limited number of cyber security controls and those

controls were implemented inconsistently at each FCF.

Stakeholder Interactions on the Final Regulatory Basis:

After NRC staff review of FCF licensee voluntary cyber security measures and an analysis of stakeholder comments on the draft regulatory basis, the staff proceeded to develop the final regulatory basis. The staff held four public meetings to discuss the proposed graded, consequence-based approach for cyber security at FCFs and receive stakeholder feedback. The four public meetings were held on October 22, 2015 (ADAMS Accession Nos. ML15288A514 and ML15293A086); December 10, 2015 (ADAMS Accession No. ML15356A357); February 18, 2016 (ADAMS Accession No. ML16054A160); and March 17, 2016 (ADAMS Accession No. ML16092A124). Feedback received at these meetings informed the staff's development of the final regulatory basis, which was completed on March 24, 2016 (ADAMS Accession No. ML15355A466). The final regulatory basis document was made publicly available in a *Federal Register* notice dated April 12, 2016 (81 FR 21449).

Stakeholder Interactions on the Draft Proposed Rule:

After completion of the final regulatory basis, the NRC staff developed draft proposed rule language. The staff held four public meetings to present the preliminary draft proposed rule text, related guidance, and projected costs for implementation of the proposed rule. These meetings were held on: May 19, 2016 (ADAMS Accession No. ML16155A442); August 25, 2016 (ADAMS Accession No. ML16271A019); October 12, 2016 (ADAMS Accession No. ML16306A050); and March 29, 2017 (ADAMS Accession No. ML17100A111). The staff considered stakeholder feedback provided at the public meetings and in an NEI letter dated October 19, 2016 (ADAMS Accession No. ML16315A290), to refine the rulemaking documents and inform the projected cost estimates for implementation of the proposed rule. In addition,

staff continued to make stakeholders aware of the rulemaking as a part of the NRC's 11th Fuel Cycle Information Exchange conference on June 14, 2017. During the "Cyber Security Roadmap" presentation, staff discussed the proposed rule and its status.

Advisory Committee on Reactor Safeguards (ACRS) Interactions on the Draft Proposed Rule:

The ACRS reviews NRC regulatory matters in order to advise the Commission, in part, on the adequacy of proposed safety standards pertaining to production and utilization facilities. On November 2, 2016, the NRC staff briefed the 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), 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; and

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 (CRGR) Interactions on the Draft Proposed Rule:

The CRGR is an advisory committee that reviews proposed generic backfits that are to be imposed on nuclear power plants and selected nuclear materials facilities that are licensed by the NRC. The committee's primary responsibilities are to guide and assist the NRC's program offices in implementing the Commission's backfit policy. The proposed rule would affect FCFs licensed under 10 CFR part 70 that are afforded backfitting protection, in accordance with 10 CFR 70.76, "Backfitting." 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 CRGR review and endorse the proposed rule package and associated draft regulatory guide for cyber security at FCFs. On June 27 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, draft backfit analysis, "Draft Backfit Analysis and Documented Evaluation for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR 73.53)" (ADAMS Accession No. ML17018A221), and guidance document were comprehensive and thorough. The CRGR members indicated that the staff's graded approach and rationale supported thoughtful decisionmaking 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; and

2) Provide appropriate clarification of the regulatory bases for FCFs licensed under 10 CFR 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 and regulatory analyses. 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.

IV. Discussion

A. What action is the NRC taking?

The NRC is proposing amendments to its regulations in 10 CFR part 73, “Physical Protection of Plants and Materials,” and conforming amendments to other regulations, to establish new cyber security requirements for FCF licensees. The proposed rule, if adopted, would require FCF licensees to establish, implement, and maintain a cyber security program designed to detect, protect against, and respond to a cyber attack capable of causing a consequence of concern, thereby increasing the overall safety and security at FCFs. The cyber security program would be designed to ensure that FCF licensees protect certain digital assets at their facilities that if compromised could adversely impact the public health and safety and common defense and security. In addition, the NRC is issuing new draft guidance, DG-5062, “Cyber Security Programs for Nuclear Fuel Cycle Facilities,” pertaining to the implementation of the proposed requirements in this rulemaking.

B. Why is this action necessary?

The NRC does not currently have a comprehensive regulatory framework for addressing cyber security at FCFs. Subsequent to the events of September 11, 2001, the NRC issued ICM Orders that required FCF licensees to implement measures to enhance cyber security. These orders required FCF licensees to evaluate computer and communications networks, and address safety and security vulnerabilities as necessary. Additionally, in Section 651 of the EPAct 2005, Congress directed the Commission to initiate a rulemaking to revise the DBTs set forth in 10 CFR 73.1. The Commission was specifically directed to consider a potential cyber threat in the DBT rulemaking. In 2007, in response to this direction, the Commission promulgated a rulemaking entitled “Design Basis Threat” (72 FR 12705; dated March 19, 2007), revising 10 CFR 73.1 to explicitly include a cyber security threat as an element of the DBTs. In accordance with 10 CFR 73.20, Category I FCF licensees must maintain a physical protection system to protect against both DBTs.

Since the issuance of the ICM Orders and the 2007 DBT rulemaking, the threats to digital assets have increased both globally and nationally. Cyber attacks have increased in number, become more sophisticated, resulted in physical consequences, and targeted digital assets similar to those used by FCF licensees. The NRC staff has determined that the general cyber security performance objectives in the ICM Orders and the DBTs do not provide specific requirements or guidance on how FCF licensees are to meet those general performance objectives. Therefore, the proposed rule would require FCF licensees to develop and implement a cyber security program to address the evolving cyber security threat at FCFs. In particular, the proposed rule would require FCF licensees to analyze potential consequences of concern, identify appropriate VDAs that if compromised by a cyber attack, would result in a consequence of concern, and implement appropriate cyber security controls to protect those VDAs.

In 2010 and again in 2015, the NRC staff reviewed voluntary cyber security measures at the various types of FCFs (Category I FCFs, Category III FCFs, and 10 CFR part 40 uranium hexafluoride conversion facilities). The reviews were conducted to determine how the licensees for these facilities protect their digital assets from a cyber attack and evaluate whether additional cyber security requirements are needed to protect public health and safety and promote common defense and security.

As a result of its interactions with FCF licensees, the NRC staff identified that licensees rely upon digital assets for the performance of important safety, security, and safeguards functions. If the compromise [2] of one of these digital assets were to go undetected and unresolved, the cyber attack could directly result in a safety consequence of concern (i.e., an active consequence of concern) or compromise a function needed to prevent an event associated with a consequence of concern (i.e., a latent consequence of concern). The proposed rule would require FCF licensees to establish, implement, and maintain a cyber security program that, if implemented in accordance with the proposed rule's requirements, would meet the cyber security performance objectives set forth in the ICM Orders and the DBTs. The program would promote common defense and security and provide reasonable assurance that the public health and safety remain adequately protected against the evolving risk of cyber attacks.

C. Who would this action affect?

The proposed requirements would apply to each applicant or licensee that is or plans to

[2] "Compromise" means that the digital asset loses confidentiality, integrity, or availability of data or function. Note that the term "compromise" encompasses a broader meaning than the term "failure." Failure means that the intended function is not performed. This compromise of a digital asset could include the failure of the intended function.

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 special nuclear material, 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 applicants or licensees subject to 10 CFR 70.60 or those subject to 10 CFR part 40 for operation of a uranium hexafluoride conversion or deconversion facility.

The proposed rule takes into account hazards specific to the different types of FCF licensees: 1) 10 CFR part 70 licensees authorized to possess or use a formula quantity of SSNM as defined in 10 CFR 73.2 (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 and deconversion facility licensees).

D. Why are voluntary actions and existing cyber security requirements for FCFs not sufficient?

During the period 2010 to 2015, the NRC staff conducted assessments of FCF licensees' voluntary cyber security measures to determine how these licensees protect against a cyber attack. The staff's assessments specifically looked at digital assets that performed,

supported, or were associated with safety, security, and safeguards functions.[3] The staff determined that digital assets performing these functions if compromised by a cyber attack, would result in a consequence of concern and may require additional protection from a cyber attack. Furthermore, the staff identified that licensee voluntary cyber security measures lacked a comprehensive analysis of cyber security vulnerabilities and, in certain cases, addressed only a limited number of cyber security threats. Because the licensees' actions are voluntary and are not included in their security plans or licenses as a license condition, the NRC has no oversight, inspection, or enforcement authority to ensure the implementation of these cyber security actions at FCFs.

In accordance with 10 CFR 73.20, Category I FCF licensees must maintain a physical protection system designed to protect against the DBTs (i.e., radiological sabotage and theft or diversion of SSNM). Both DBTs require consideration of a cyber attack by adversaries. However, the NRC's current physical protection regulations in 10 CFR part 73 do not provide specific requirements or guidance for addressing a cyber attack on Category I FCFs.

The ICM Orders contained a generic requirement to consider cyber security and address safety and security vulnerabilities "as necessary." The relevant NRC guidance focused on the impact of a cyber attack on emergency response and offsite support. In general, licensees responded that a cyber attack would have a minimal impact on emergency response and offsite support, and that the licensees would monitor network security going forward. These cyber security commitments were deemed adequate for FCF licensees given the cyber threat environment at that time.

With the evolution in the cyber threat to FCF licensees since the ICM Orders were

---

[3] Safeguards functions are related to material control and accounting of SNM and are further discussed in Section 3.4.4 of the final regulatory basis for cyber security at FCFs (ADAMS Accession No. ML15355A466).

issued and the DBT rule was revised, the NRC has determined that specific cyber security requirements for FCF licensees are warranted. Therefore, the NRC staff has developed this proposed rule that would require FCF licensees to analyze potential consequences of concern; identify appropriate VDAs that if compromised by a cyber attack, would result in a consequence of concern; and implement adequate cyber security controls to protect those VDAs.

E. Why not apply the existing requirements from 10 CFR 73.54 to FCF licensees?

The cyber security requirements in 10 CFR 73.54 were developed specifically for nuclear power reactors to address the types of digital systems and hazards common to these facilities. Power reactor facilities in the United States typically utilize similar types of systems, structures, and components. Accordingly, it is appropriate to have a common set of cyber security requirements for these facilities. Therefore, all operating nuclear power reactor licensees are subject to the same set of requirements in 10 CFR 73.54.

By contrast, FCFs represent a broad spectrum of facility types, processes, and potential consequences of concern that could result from a cyber attack. For example, the type and severity of consequences caused by a cyber attack compromising a digital asset at a Category I FCF may be much different from the consequences of such an attack at a Category III FCF, or at a uranium hexafluoride conversion or deconversion facility. Furthermore, the potential consequences of a successful cyber attack at a FCF could be significantly different from the potential consequences of a successful cyber attack at a power reactor facility. Given the scope of the differences among FCFs as compared with power reactors, the NRC staff determined that the single set of cyber security requirements developed for commercial nuclear power reactors was not appropriate for FCF licensees.

Accordingly, and consistent with Commission direction, the NRC staff developed a proposed rule that would establish graded, consequence-based requirements for the protection

of digital assets at FCFs to provide the appropriate level of protection at each facility. The proposed rule reflects several insights that the staff gained from reviewing the development and implementation of 10 CFR 73.54. Based on these insights, the proposed rule for cyber security at FCFs incorporates the following characteristics: 1) adopting a graded, consequence-based approach for determining appropriate cyber security requirements based on facility type; 2) defining a specific and consequence-based process for identifying digital assets that are within the scope of the regulatory requirements of the rule; 3) establishing a risk-informed screening process to identify in-scope digital assets whose function is maintained by an alternate means and, therefore, do not require additional cyber security controls; 4) adding flexibility within the proposed rule to allow licensees to satisfy the performance objectives by applying cyber security controls through a graded, consequence-based approach, taking credit for existing programs, and using alternate controls to prevent consequences of concern; 5) ensuring licensee programs and processes meet regulatory requirements prior to focusing on technical implementation; and 6) establishing an implementation schedule with firm deadlines.

F. What effect may PRM-73-18 have on the proposed rule?

On June 12, 2014, NEI submitted to the NRC a petition for rulemaking (PRM), 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 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 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. 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.

G. What are the requirements of the proposed cyber security program?

The NRC staff has developed a proposed rule that utilizes a graded, consequence-based approach for addressing the protection of digital assets at FCFs. The proposed rule would require FCF licensees 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. 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 VDAs that require protection; 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 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 cyber security program would provide for the identification of digital assets that if compromised by a cyber attack, would result in a consequence of concern. Licensees would need to document the process for identifying those digital assets (i.e., VDAs) that, if

compromised by a cyber attack, would result in a consequence of concern. Licensees would have to implement cyber security controls for the protection of identified VDAs and develop implementing procedures that document the measures taken to address the performance specifications associated with the cyber security controls. Licensees would also need to provide temporary compensatory measures (if needed) to meet the cyber security program performance objectives when the cyber security controls are degraded.

The proposed rule would require FCF licensees to list, in the cyber security plan, the cyber security controls for the types of consequences of concern applicable to their facility. The NRC has developed a draft regulatory guide that sets forth a list of acceptable cyber security controls that licensees may choose to adopt. The NRC staff's development of this list of cyber security controls was informed by the NIST cyber security documents and standards discussed in Section III.D of this document. For additional information about the draft regulatory guide, see Section XIII, "Availability of Guidance," of this document.

The proposed rule includes requirements for event reporting and tracking. First, the requirements of the proposed rule would supplement existing event reporting requirements by requiring FCF licensees to 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. Licensees could provide this information as part of the initial event report or in a subsequent report, if the licensee does not discover until later that the event was the result of a cyber attack. Secondly, licensees would need to internally record and track to resolution a discovered failure, compromise, vulnerability, or degradation that results in the decrease in effectiveness of a cyber security control or a cyber attack that compromises a VDA. Although these occurrences need to be recorded, tracked to resolution, and documented, the licensee does not need to formally report these occurrences to the NRC.

H. How does the proposed rule use a graded, consequence-based approach for the protection of digital assets?

The proposed rule would use a consequence-based approach by identifying specific consequences of concern that take into account the various potential hazards at the different types of FCFs. Not all types of consequences of concern are applicable to each FCF, and licensees would only need to provide protection against a cyber attack capable of causing a consequence of concern applicable to their facility. For example, the consequence of concern associated with theft and diversion of SSNM would only be applicable to Category I FCF licensees because they are the only FCF licensees that possess or use SSNM.

The proposed rule would apply a graded, consequence-based approach to cyber security controls by requiring licensees to only protect a VDA at a level commensurate with the consequence of concern associated with that VDA. The proposed rule recognizes that the cyber security controls applicable to a particular VDA may vary depending on the nature and severity of the consequence of concern at a particular facility. For example, at a Category I FCF, to address the consequence of concern for safeguarding formula quantities of SSNM, the proposed rule would require application of controls to the VDAs protecting the SSNM that are more stringent than those applied to VDAs protecting SNM of moderate strategic significance at a Category II FCF. If a VDA is associated with more than one consequence of concern, that VDA would have to be protected at a level commensurate with the most severe consequence.

I. What is a consequence of concern?

A consequence of concern, as defined in the proposed rule, is an event that occurs as a result of the compromise of a VDA that has the potential to adversely impact public health and safety or common defense and security. The provisions of the proposed rule would require FCF licensees to identify and document those digital assets that, if compromised by a cyber attack,

would result in a consequence of concern. Such digital assets that are then determined to be VDAs must be protected by the application of appropriate cyber security controls. Therefore, the concept of consequence of concern defines and determines the scope of digital assets that must be protected at each FCF.

In the proposed rule, the NRC staff has identified four types of consequences of concern that a FCF licensee's cyber security program would need to protect against:

1) latent – DBT;
2) latent – safeguards;
3) active – safety; and
4) latent – safety and security.

J. What are the differences between 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). When there is a latent consequence of concern, the compromised digital asset is no longer available to provide the function needed to prevent the secondary event. The combination of the compromise of the digital asset from the cyber attack (i.e., the latent consequence of concern) and the secondary event must both occur for there to be a significant impact on public health and safety or common defense and security.

K. How are the consequences of concern used in the proposed rule?

The proposed rule would establish thresholds for each of the four types of consequences of concern defined in the proposed rule. The NRC staff has determined that these consequences of concern could result in the following: radiological and chemical exposures; theft or diversion of SSNM and radiological sabotage as stated in 10 CFR 73.1(a) (applicable only to Category I FCF licensees); loss of nuclear material control and accounting safeguards (applicable only to Category I and II FCF licensees); and loss of classified information or matter. The thresholds for each consequence of concern would align with existing regulatory requirements.

Consequences of concern that address security and safeguards functions:

The provisions in 10 CFR part 73 provide for the physical protection of plants and materials. Section 73.20 includes a requirement for Category I FCF licensees to establish a physical protection system to protect against the DBTs of theft or diversion of SSNM and radiological sabotage. Section 73.45 describes the performance capabilities that Category I FCF licensees must establish for the site's physical protection system. Section 73.46 provides the specific elements that Category I FCF licensees must include in their physical protection system to meet the general performance objective and performance capabilities in 10 CFR 73.20 and 73.45. Section 73.67 provides general performance objectives and requirements for Category II FCF licensees to protect SNM of moderate strategic significance. Some FCF licensees currently use digital assets to meet the performance objectives and requirements of these sections, and other FCF licensees may do so in the future.

In 10 CFR part 74, "Material Control And Accounting of Special Nuclear Material," FCF licensees (Category I and II FCF licensees) are required to implement and maintain a material control and accounting system (safeguards). The physical protection and safeguards programs work together to create an integrated and complementary security approach that results in more

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.

Pursuant to 10 CFR part 95, “Facility Security Clearance and Safeguarding of National Security Information and Restricted Data,” FCF licensees (i.e., Category I and Category III enrichment FCF licensees) are required to establish procedures for obtaining facility security clearance and for safeguarding security information or matter, received or developed in conjunction with licensed activities. The classified systems and networks that process and store this information must have cyber security controls approved by the authorizing official at the U.S. Department of Energy (DOE). However, the digital assets associated with the physical security of this classified information or matter (e.g., door alarms) fall within the regulatory purview of the NRC. Some FCF licensees currently utilize digital assets to physically protect classified information or matter, and other FCF licensees may do so in the future.

There are two consequences of concern that are specific to security and safeguards functions:

1) Latent consequences of concern – DBT:

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

2) Latent consequences of concern – safeguards:

A latent consequence of concern – safeguards is only applicable to a FCF authorized to possess or use SNM of moderate strategic significance (i.e., Category II FCF). This 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 end result is that the security function cannot be relied upon when required.

Consequences of concern that address safety functions:

The proposed rule would be applicable to FCF licensees that must also comply with the requirements of 10 CFR 70.62, “Safety program and integrated safety analysis.” The provisions of 10 CFR 70.62 require the development and maintenance of a safety program that demonstrates compliance with 10 CFR 70.61, “Performance requirements,” which pertains to accident prevention and mitigation. One element of the safety program consists of conducting an integrated safety analysis (ISA). The FCF licensees or applicants are required to identify in their ISA: 1) radiological hazards related to possessing or processing licensed material at its facility; 2) chemical hazards of licensed material and hazardous chemicals produced from licensed material at its facility; 3) facility hazards that could affect the safety of licensed materials and present an increased radiological risk; 4) potential accident sequences caused by process deviations or other events internal to the facility and credible external events; 5) the consequence and likelihood of occurrence of each potential accident sequence identified; and 6) each item (i.e., engineered or administrative control) relied on for safety (IROFS) to support compliance with the performance requirements of 10 CFR 70.61.

The FCF licensees subject to 10 CFR 70.62 are required to implement IROFS to

mitigate or prevent the risk of high consequence events identified in 10 CFR 70.61(b) and the risk of intermediate-consequence events identified in 10 CFR 70.61(c). The safety program must also ensure that each IROFS [4] is available and reliable to perform its intended function when needed. If not adequately protected, these IROFS have the potential to be compromised by a cyber attack and may not be available or reliable during an event. This compromise would have the potential to result in a safety consequence of concern. Most FCF licensees currently rely upon digital assets integrated into their safety program, and other FCF licensees may do so in the future.

There are two consequences of concern that relate to safety functions:

1) Active consequences of concern – safety:

An active consequence of concern – safety is 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.[5]

2) Latent consequences of concern – safety and security:

A latent consequence of concern – safety and security involves the compromise of a safety or security function due to a cyber attack. The attack renders one or more digital assets 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

---

[4] Also referred to as plant features and procedures by one FCF licensee.

[5] The thresholds for the safety consequences of concern in the proposed rule are informed by the requirements in 10 CFR 70.61(b). Note that the safety consequences of concern in the proposed rule are derived from the high consequence event thresholds for members of the public in 10 CFR 70.61(b), but as used here are applicable to both the worker and the public.

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 (10 CFR part 95). In addition, material control and accounting functions whose compromise could lead to a latent safety consequence of concern, would need to be protected from a cyber attack.

L. How does the licensee identify digital assets that if compromised by a cyber attack, would result in a consequence of concern?

Under the proposed rule, each FCF licensee would be required to identify the types of consequences of concern applicable to its facility. The licensee would then be required to identify digital assets that if compromised by a cyber attack, would result in a consequence of concern. In identifying these digital assets, a licensee may use any existing resources to support the identification process, such as ISAs, process hazards analyses, physical security plan, material control and accounting plan, security orders, previously considered impacts from a cyber attack, any site or vulnerability analyses, or other safety or security information.

The FCF licensee would be required to maintain a record of those digital assets that if compromised by a cyber attack, would result in a consequence of concern. The list would include the name and physical location of each application, device, system, or network identified as a digital asset and which of the four consequences of concern are applicable if a compromise of the digital asset were to occur.

M. How does the licensee determine if the identified digital assets are vital?

A licensee must first identify those digital assets that if compromised by a cyber attack, would result in a consequence of concern. The licensee must then determine if an alternate means that is protected from a cyber attack exists to prevent the consequence of concern. If no alternative means of protection exists, then the digital asset is a VDA and must be protected by appropriate cyber security controls. As part of this analysis, licensees would also identify associated support systems for VDAs that, if compromised by a cyber attack, could lead to a consequence of concern. Licensees would also be required to establish and maintain implementing procedures to document the measures taken to address the cyber security controls for the VDAs.

N. What is meant by alternate means?

An alternate means is a credible and effective substitute for the function performed by a digital asset that prevents a consequence of concern. The alternate means must be able to independently prevent the consequence of concern associated with the digital asset. An acceptable alternate means prevents the identified consequence of concern and is: protected from a cyber attack; sufficiently reliable and adequately implemented consistent with other safety features; properly maintained; activated in a timely manner to prevent the identified consequence of concern; and implemented with appropriate and adequate resources. Furthermore, an acceptable alternate means would not be adversely impacted by a cyber attack exploiting multiple attack vectors (i.e., a multi-node attack) or the potential cumulative effects that could result from the simultaneous compromise of several digital assets by a cyber attack. An acceptable alternate means does not contribute to other vulnerabilities or lead to a consequence of concern.

If an alternate means is identified for a digital asset, then that digital asset would not be considered vital and no cyber security controls would be required. For example, a pressure

relief valve that releases material into a safe holding tank may be considered an alternate means for a digital asset preventing over-pressurization of a process line, because the valve would prevent a release if the digital asset were compromised and failed to perform its function. Similarly, a routine security patrol may be considered an alternate means for a digital camera if the patrol performs the same detection function as the camera. The consideration of alternate means provides FCF licensees an opportunity to demonstrate how other safety and security elements provide defense-in-depth to protect against a cyber attack capable of causing a consequence of concern.

A VDA can be considered for use as an alternate means for another digital asset so long as that VDA is protected from a cyber attack. Licensees would document the basis for the determination of an acceptable alternate means. The licensee must be able to demonstrate that the alternate means prevents the consequence of concern.

O. Does the NRC recognize the accreditation of classified or unclassified systems by another Federal agency in the proposed rule?

The proposed rule provides an exception for digital assets on classified systems accredited by another Federal agency. The proposed rule would not require any additional cyber security analysis or controls for these digital assets. The NRC staff has determined that the requirements for accreditation of classified systems by another Federal agency provide acceptable protection of digital assets on classified systems at FCFs.

The NRC staff is continuing discussions with the three Federal entities (Oak Ridge Operations Office, National Nuclear Security Administration (NNSA) Headquarters, and NNSA's Naval Reactors Office) involved with the accreditation of unclassified systems at FCFs. The three DOE entities are expected to complete a revision of their respective cyber security specifications for accreditation of unclassified systems at FCFs in 2017. The staff plans to

assess the protection provided to digital assets on unclassified systems by DOE's revised cyber security requirements once they have been finalized.

P. Is the NRC considering a phased implementation of the proposed rule?

As directed by the Commission in the SRM for SECY-14-0147, the NRC staff is considering an 18-month implementation period. Within 180 days after publication of the final rule or 180 days prior to possessing licensed material, whichever is later, the proposed rule would require each FCF licensee to submit, through an application for amendment of its license, a cyber security plan that satisfies the requirements of 10 CFR 73.53, "Requirements for cyber security at nuclear fuel cycle facilities," for NRC review and approval. In addition, each FCF applicant who has submitted an application to the NRC prior to the effective date of the final rule would be required to amend their application to include a cyber security plan that satisfies the requirements of 10 CFR 73.53 for NRC review and approval. Within 150 days of submission, the NRC would review the license amendment request and the associated cyber security plan. If all appropriate regulatory requirements are met, the cyber security license amendment would be granted with specific implementation dates specified in the NRC's written approval of the cyber security plan.

The NRC staff is considering having two phases reflected in the implementation dates: 1) Within 6 months of NRC approval of the cyber security plan, each FCF licensee would identify VDAs and complete the associated documentation; and 2) Within 18 months of NRC approval of the cyber security plan, each licensee would fully implement the cyber security plan. For the phased implementation timeline described above, the NRC would perform an inspection upon completion of each of the two milestones.

Q. What should I consider as I prepare my comments for submission to the NRC?

When submitting your comments:

1) Identify the rulemaking ((Docket ID: NRC-2015-0179) and Regulation Identifier Number (RIN 3150-AJ64).

2) Explain why you agree or disagree; suggest alternative and substitute language for your requested changes.

3) Describe any assumptions and provide any technical information or data that you used.

4) If you estimate potential costs or burdens, explain how you arrived at your estimate in sufficient detail to allow for it to be reproduced.

5) Provide specific examples to illustrate your concerns and suggest alternatives.

6) Explain your views as clearly as possible.

7) Make sure to submit your comments by the comment period deadline.

V. Discussion of the Proposed Amendments by Section

The proposed rule would add one new section to 10 CFR part 73 (10 CFR 73.53) and make conforming changes to 10 CFR parts 40 (10 CFR 40.4, 40.31, and 40.35), 70 (10 CFR 70.22 and 70.32) and 73 (10 CFR 73.8 and 73.46).

10 CFR 40.4 – Definitions

This section would be revised to add a new definition for the term “Uranium hexafluoride conversion or deconversion facility.” This definition is intended to clarify that such a facility is one that engages in hexafluoride conversion or deconversion as part of its principal activities, and does not include those facilities that may engage in incidental hexafluoride conversion or deconversion in support of other activities such as uranium enrichment or fuel fabrication.

10 CFR 40.31 – Application for specific licenses

This section would be revised to add a paragraph (n) to require each applicant for a uranium hexafluoride conversion or deconversion facility license under 10 CFR part 40, "Domestic Licensing of Source Material," to submit a cyber security plan that meets the requirements in 10 CFR 73.53.

10 CFR 40.35 – Conditions of specific licenses issued pursuant to 10 CFR 40.34

This section would be revised to add a paragraph (g) to require fuel cycle licensees that possess source material for the production, conversion, or deconversion of uranium hexafluoride to submit cyber security plan changes that would result in a decrease in effectiveness in the plan, as a license amendment request for NRC review and approval. The NRC review would involve a determination of whether or not the cyber security plan changes maintain compliance with regulatory requirements. The provision would allow licensees to make changes to the cyber security plan without NRC review, approval, and license amendment, provided the changes do not decrease the effectiveness of the plan. In addition, the proposed provision would establish recordkeeping requirements for the cyber security plan and its changes.

10 CFR 70.22 – Contents of application

This section would be revised to add a paragraph (o) to require each application for a license to 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, to include a cyber security plan that demonstrates how the applicant plans to meet the requirements of 10 CFR 73.53. The provision also would specifically exclude decommissioning activities performed pursuant to other applicable Commission regulations.

10 CFR 70.32 – Conditions of licenses

This section would be revised to add a paragraph (f) to require cyber security plan changes that would result in a decrease in effectiveness in the plan to be submitted as a license amendment request for NRC review and approval. The NRC review would involve a determination of whether or not the cyber security plan changes maintain compliance with regulatory requirements. The provision would allow licensees to make changes to their cyber security plans without NRC review, approval, and license amendment, provided the changes do not decrease the effectiveness of the plan. In addition, the proposed provision would establish recordkeeping requirements for the cyber security plan and its changes.

10 CFR 73.8 – Information collection requirements: Office of Management and Budget (OMB) approval

Paragraph (b) would be revised to indicate that 10 CFR 73.53 contains information collection requirements.

10 CFR 73.46 – Fixed site physical protection systems, subsystems, components, and procedures

Paragraph (g)(6) would be revised to add cyber security program review requirements to the current annual security program review requirements for Category I FCF licensees.

10 CFR 73.53 – Cyber security for fuel cycle facilities

This new section would contain cyber security program requirements for fuel cycle facility licensees. Paragraph (a) would identify the licensees and applicants for which the requirements apply, and require licensees to submit a cyber security plan for NRC review and approval. Paragraph (b) would set forth the program performance objectives that govern FCF licensee cyber security programs. To meet these program performance objectives, FCF licensees would be required to establish, implement, and maintain a cyber security program with the capability 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 be designed to protect against. Paragraph (d) would establish the required elements of a licensee cyber security program, including a cyber security team, identification of VDAs, and the application of cyber security controls to VDAs in accordance with the documented implementing procedures. Paragraph (e) would identify the requirements to establish, implement, and maintain a cyber security plan. Paragraph (f) would establish a requirement for licensees to utilize configuration management for the cyber security program. Paragraph (g) would establish a requirement for licensees to perform periodic reviews of the cyber security program.[6] Paragraph (h) would establish requirements for cyber security event reporting and tracking. Paragraph (i) would establish recordkeeping requirements.

VI. Agreement State Compatibility

[6] Category I FCF licensees would be required to conduct cyber security program reviews annually, consistent with current security program review requirements. All other FCF licensees would be required to conduct cyber security program reviews every 36 months.

Under the ‘‘Policy Statement of Adequacy and Compatibility of Agreement States Programs,’’ approved by the Commission on June 20, 1997, and published in the *Federal Register* (62 FR 46517; September 3, 1997), all changes to the NRC regulations in this proposed rule are classified as Category ‘‘NRC’’ for compatability purposes. The NRC program elements in Category “NRC” are those that relate directly to areas of regulation reserved to the NRC by the AEA, or the provisions of 10 CFR. Thus, Agreement States should not adopt these program elements.

VII. Regulatory Flexibility Certification

As required by the Regulatory Flexibility Act of 1980, 5 U.S.C. 605(b), the Commission certifies that this rule would not, if adopted, have a significant economic impact on a substantial number of small entities. Although the NRC believes the companies that own the facilities affected by the proposed rule do not fall within the scope of the definition of “small entities” set forth in the Regulatory Flexibility Act or the size standards established by the NRC (10 CFR 2.810), the NRC is seeking public comment on its certification determination. Specifically, the NRC is seeking public comment as to how the proposed regulation would affect small entities and how the regulation may be tiered or otherwise modified to impose less stringent requirements on them while still promoting common defense and security and adequately protecting the public health and safety. Comments on how the regulation could be modified to take into account the differing needs of small entities should specifically discuss:

1) The licensee’s size and how the proposed regulation would impose a significant economic burden on the licensee as compared to the economic burden on a larger licensee;

2) How the proposed regulations could be modified to take into account the licensee’s differing needs or capabilities;

3) The benefits that would accrue or the detriments that would be avoided if the proposed regulations were modified as suggested by the licensee;

4) How the proposed regulation, as modified, would more closely equalize the impact of NRC regulations or create more equal access to the benefits of Federal programs as opposed to providing special advantages to any individual or group; and

5) How the proposed regulation, as modified, would still promote common defense and security and adequately protect public health and safety.

Comments may be submitted as indicated under the ADDRESSES caption of this document.

VIII. Regulatory Analysis

For the proposed rule, the NRC has prepared the draft regulatory analysis to examine the benefits and costs of the alternatives considered. The draft regulatory analysis measures the incremental costs of the proposed rule relative to a "baseline" that reflects anticipated behavior in the event the NRC undertakes no additional regulatory action. The analysis evaluates benefits and costs associated with four affected attributes: industry implementation, industry operations, NRC implementation, and NRC operations. Because some of the benefits associated with affected attributes are not easily susceptible to quantification, the NRC staff performed a qualitative assessment of these attributes, consistent with the guidance provided in NUREG/BR-0058, Revision 4, "Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission," dated September 2004, and NUREG/BR-0184, "Regulatory Analysis Technical Evaluation Handbook, dated January 1997 (ADAMS Accession No. ML111290858). The NRC requests public comment on the draft regulatory analysis. In particular, the NRC requests comments on the benefits and costs associated with implementing the proposed rule. The draft

regulatory analysis is available as indicated in the “Availability of Documents” section of this document. Comments on the draft regulatory analysis may be submitted to the NRC as indicated under the ADDRESSES section of this document.

IX. Backfit Analysis

The proposed rule would affect fuel cycle facilities licensed under 10 CFR parts 40 and 70. Of these entities, only FCFs licensed under 10 CFR part 70 and subject to the requirements of subpart H to 10 CFR part 70 are afforded backfitting protection, in accordance with 10 CFR 70.76, “Backfitting.” As documented in “Draft Backfit Analysis and Documented Evaluation for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR 73.53)” (ADAMS Accession No. ML17018A221), the NRC staff has determined that the proposed rule would constitute a backfit. This backfit is justified, in part, based on adequate protection and in part based on a cost-justified substantial increase in overall protection. The adequate protection exception applies to those provisions of the proposed rule that are associated with: 1) protecting against the DBTs, and 2) protecting against the loss or unauthorized disclosure of classified information or matter (10 CFR part 95). These provisions of the proposed rule correspond to the security and safeguards consequences of concern. The provisions of the proposed rule that are cost-justified correspond to the safety consequences of concern.

As further discussed in the draft backfit analysis, the provisions of the proposed rule pertaining to adequate protection are necessary because they clarify and codify current Commission direction to protect against DBT and safeguards events.

The NRC performed a backfit analysis with respect to the provisions of the proposed rule associated with the safety consequences of concern in accordance with 10 CFR 70.76 to determine if there is a substantial increase in the overall protection of the public health and

safety or common defense and security to be derived from the backfit and, if so, whether the direct and indirect costs of implementation are justified in view of this increased protection. As documented in the draft backfit analysis, the NRC finds that the provisions of the proposed rule associated with the safety consequences of concern provide a cost-justified substantial increase in overall protection because the benefits of these provisions exceed the costs associated with their implementation.

X. Cumulative Effects of Regulation

The NRC has established the cumulative effects of regulation (CER) initiative in the development of rulemakings. The CER initiative pertains to the challenges that licensees, or other impacted entities (such as State partners), may face when implementing new regulatory positions, programs, and requirements (e.g., rules, generic letters, backfits, and inspections). The CER is an organizational effectiveness challenge that results from a licensee or impacted entity implementing a number of complex positions, programs, or requirements within a limited implementation period and with available resources (which may include limited available expertise to address a specific issue). The NRC is specifically requesting comments on the cumulative effects that may result from the proposed rule. Please consider answering the following questions to assist the NRC in evaluating potential CER impacts related to the proposed rule:

1) In light of any current or projected CER challenges, what should be a reasonable effective date, compliance date, or submittal date(s) from the time the final rule is published to the actual implementation of any new proposed requirements including changes to programs, procedures, or the facility?

2) If current or projected CER challenges exist, what should be done to address this

situation (e.g., if more time is required to implement the new requirements, what period of time would be sufficient, and why such a time frame is necessary)?

3) Do other (NRC or other agency) regulatory actions (e.g., orders, generic communications, license amendment requests, and inspection findings of a generic nature) influence the implementation of the proposed rule's requirements?

4) Are there unintended consequences? Does the proposed rule create conditions that would be contrary to the proposed rule's purpose and objectives? If so, what are the unintended consequences, and how should they be addressed?

5) Please comment on the resources estimated by the NRC in the regulatory analysis that supports the proposed rule.

Comments may be submitted as indicated under the ADDRESSES caption of this document.

XI. Plain Writing

The Plain Writing Act of 2010 (Pub. L. 111-274) requires Federal agencies to write documents in a clear, concise, and well-organized manner. The NRC has written this document to be consistent with the Plain Writing Act as well as the Presidential Memorandum, "Plain Language in Government Writing," published June 10, 1998 (63 FR 31883). The NRC requests comment on this document with respect to the clarity and effectiveness of the language used.

XII. Environmental Assessment and Proposed Finding of No Significant Environmental Impact: Availability

The NRC 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 this rule and guidance, if adopted, would have no significant environmental impacts, and therefore do not warrant the preparation of an environmental impact statement. The proposed rule and guidance pertain to requirements for FCF licensees to establish, implement, and maintain a cyber security program designed to promote common defense and security and protect public health and safety. Under the proposed requirements, licensees would establish and maintain a cyber security program to implement a graded, performance-based regulatory framework for the protection of digital assets from a cyber attack capable of causing the consequences of concern identified in the proposed rule. The determination of this environmental assessment is that there would be no significant offsite impact to the public from this action. The draft environmental assessment, entitled "Draft Environmental Assessment and Finding of No Significant Impact for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR 73.53)," can be found in ADAMS under Accession No. ML17026A102.

XIII. Paperwork Reduction Act Statement

The proposed rule contains new or amended collections of information subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq). The proposed rule has been submitted to the OMB for review and approval of the information collections.

- *Type of submission, new or revision:* Revision

- *The title of the information collection:* 10 CFR part 73, "Cyber Security at Fuel Cycle Facilities"

- *The form number if applicable:* NA

- *How often the collection is required or requested:* Each NRC 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 special nuclear material, 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 would be required to submit a cyber security plan for review and approval. This would be considered a one-time reporting requirement. Each FCF licensee would be required to submit to the NRC a license amendment request for any change that would decrease the effectiveness of the cyber security plan. At least every 12 months, Category I FCF licensees would be required to review and document the effectiveness of their cyber security program. These annual records would include the documentation of any minor changes to cyber security plans. All other FCF licensees would be required to review and document the effectiveness of the cyber security program at least every 36 months. Each FCF licensee would be required to inform the NRC Operations Center within 1 hour of discovery that an event requiring notification under existing reporting regulations is the result of a cyber attack. This provision would also require FCF licensees to, within 24 hours of discovery, record and track to resolution the failure, compromise, vulnerability, or degradation that results in a decrease in effectiveness of a cyber security control for a VDA. Category I and II FCF licensees would be required to record, within 24 hours of discovery, if a cyber attack compromised a VDA associated with certain safeguards consequences of concern.

- *Who will be required or asked to respond:* Each NRC 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 special nuclear material, 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 applicants or licensees subject to 10 CFR 70.60, "Applicability," or subject to 10 CFR part 40, "Domestic Licensing of Source Material," for operation of a uranium hexafluoride conversion or deconversion facility.

- *An estimate of the number of annual responses:* 8 (Note: Although there are currently 12 FCF licensees, 4 of these licensees are not currently operating or constructing a facility. As such, the number of estimated annual responses is 8.)

- *The estimated number of annual respondents:* 8

- *An estimate of the total number of hours needed annually to comply with the information collection requirement or request*: There would be a one-time reporting burden of 1,390 hours and a one-time recordkeeping burden of 7,150 hours, for a total of 8,540 hours one-time burden. The one-time burdens are based on an annualized estimate. There would be an annual reporting burden of 2,240 hours and an annual recordkeeping burden of 2,180 hours, for a total of 4,420 hours annual burden.

Abstract: The NRC is proposing a rule to incorporate protection of cyber security for FCF licensees into 10 CFR part 73, "Physical Protection of Plants and Materials," and conforming regulations. Currently, the NRC has no specific cyber security regulations for FCF

licensees. The proposed rule would add a new 10 CFR 73.53, which identifies the requirements needed to meet the cyber security program performance objectives for FCF licensees. The cyber security program performance objectives are identified in the proposed 10 CFR 73.53(b), which would require a licensee 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 rule identifies four types of consequences of concern that establish thresholds for potential events involving radiological and chemical exposures, classified information or matter, SNM of moderate strategic significance, and a formula quantity of SSNM.

The cyber security program would include: 1) establishing and maintaining a cyber security team; 2) developing a site specific cyber security plan that the licensee must submit to the NRC for review and approval; 3) conducting an analysis to identify digital assets that if compromised by a cyber attack, would result in a consequence of concern, and evaluating the digital assets to determine whether they require protection (i.e., if they are VDAs); 4) establishing and maintaining implementing procedures for VDAs that document the measures taken to address the performance specifications associated with the identified cyber security controls; 5) providing temporary compensatory measures to meet the cyber security program performance objectives when the cyber security controls are degraded; and 6) managing the cyber security program to detect, protect against, and respond to a cyber attack capable of causing a consequence of concern.

Specific requirements for reports and records related to the proposed rule are identified in the following paragraphs.

The proposed 10 CFR 73.53(g) would require Category I FCF licensees to review and document the effectiveness of the cyber security program at least every 12 months. The provision would also require all other FCF licensees to review and document the effectiveness of the cyber security program at least every 36 months.

The proposed 10 CFR 73.53(h) would require FCF licensees to inform the NRC Operations Center within 1 hour of discovery that an event requiring notification under existing reporting regulations is the result of a cyber attack. This provision would also require FCF licensees to, within 24 hours of discovery, record and track to resolution the failure, compromise, vulnerability, or degradation that results in a decrease in effectiveness of a cyber security control for a VDA. Furthermore, based upon the type of SNM used at Category I and II FCFs, licensees for these facilities would be required to record, within 24 hours of discovery, if a cyber attack compromises VDAs associated with certain safeguards consequences of concern.

The proposed 10 CFR 73.53(i) would require FCF licensees to retain the cyber security plan and supporting technical documentation demonstrating compliance with the requirements of 10 CFR 73.53 as a record. This provision would also require FCF licensees to 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 or for at least 3 years after they are superseded. The collection of this information is essential to enabling the NRC to make a determination as to the adequacy of the licensees' cyber security program to promote common defense and security and protect public health and safety.

The NRC is seeking public comment on the potential impact of the information collection(s) contained in the proposed rule and on the following issues:

1) Is the proposed information collection necessary for the proper performance of the functions of the NRC, including whether the information will have practical utility?

2) Is the estimate of the burden of the proposed information collection accurate?

3) Is there a way to enhance the quality, utility, and clarity of the information to be collected?

4) How can the burden of the proposed information collection on respondents be

minimized, including the use of automated collection techniques or other forms of information technology?

A copy of the OMB clearance package and proposed rule is available in ADAMS under Accession No. ML16323A043 or may be viewed free of charge at the NRC's PDR, One White Flint North, 11555 Rockville Pike, Room O-1 F21, Rockville, MD 20852. You may obtain information and comment submissions related to the OMB clearance package by searching on http://www.regulations.gov under Docket ID NRC-2015-0179.

You may submit comments on any aspect of these proposed information collection(s), including suggestions for reducing the burden and on the previously stated issues, by the following methods:

- **Federal rulemaking Web site:** Go to http://www.regulations.gov and search for Docket ID NRC-2015-0179.

- **Mail comments to:** FOIA, Privacy, and Information Collections Branch, Office of the Chief Information Officer, Mail Stop: T-5 F53, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001 or to Aaron Szabo, Desk Officer, Office of Information and Regulatory Affairs (3150-0002), NEOB-10202, Office of Management and Budget, Washington, DC 20503; telephone: 202-395-7315, e-mail: oira_submission@omb.eop.gov.

- Submit comments by **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]**. Comments received after this date will be considered if it is practical to do so, but the NRC staff is able to ensure consideration only for comments received on or before this date.

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the document requesting or requiring the collection displays a

currently valid OMB control number.

XIV. Availability of Guidance

The NRC is issuing a new draft regulatory guide, DG-5062, "Cyber Security Programs for Nuclear Fuel Cycle Facilities," for the implementation of the proposed requirements in this rulemaking. The draft regulatory guide is available in ADAMS under Accession No. ML16319A320. You may comment, obtain information, and access public comment submissions related to the draft regulatory guide by searching on http://www.regulations.gov under Docket ID NRC-2015-0179. In conjunction with the proposed rule, the NRC seeks public comment on DG-5062.

The draft regulatory guide is intended to describe a proposed method that the NRC staff considers acceptable for use in complying with the proposed rule for cyber security at FCFs. Because the regulatory analysis for the proposed rule provides sufficient explanation for the rule and the implementation guidance, a separate regulatory analysis was not prepared for the draft regulatory guide.

You may submit comments on this draft regulatory guidance by the following methods:

- **Federal rulemaking Web site:** Go to http://www.regulations.gov and search for Docket ID NRC-2015-0179. Address questions about NRC dockets to Carol Gallagher; telephone: 301-415-3463; e-mail: Carol.Gallagher@nrc.gov.

- **Mail comments to:** Cindy Bladey, Chief, Rules, Announcements, and Directives Branch, Office of Administration, Mail Stop: TWFN-8-D36M, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

XV. Public Meeting

The NRC plans to hold a public meeting to solicit comments on the proposed rule and the graded, consequence-based approach discussed in the draft regulatory guide. The NRC will publish a notice of the location, time, and agenda of the meeting on Regulations.gov in the Docket Folder NRC-2015-0179 (see Section II of this document for directions to subscribe for updates to the docket folder), and on the NRC's public meeting Web site within at least 10 calendar days before the meeting. Stakeholders should monitor the NRC's public meeting Web site for information about the public meeting at: http://www.nrc.gov/public-involve/public-meetings/index.cfm.

XVI. Availability of Documents

The documents identified in the following table are available to interested persons through ADAMS or the *Federal Register*, as indicated.

DOCUMENT	ADAMS ACCESSION NO. OR *FEDERAL REGISTER* CITATION
Federal Register notice of Regulatory Basis	81 FR 21449; April 12, 2016
Regulatory Basis, "Rulemaking for Cyber Security at Fuel Cycle Facilities"	ML15355A461
Draft regulatory analysis, "Draft Regulatory Analysis for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR 73.53)"	ML16320A452
Draft backfit analysis, "Draft Backfit Analysis and Documented Evaluation for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR 73.53)"	ML17018A221
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)"	ML17026A102
Draft regulatory guide DG-5062, "Cyber Security Programs for Nuclear Fuel Cycle Facilities"	ML16319A320
Design Basis Threat	72 FR 12705; March 19, 2007

Power Reactor Security Requirements Final Rule	74 FR 13926; March 27, 2009
SECY-12-0088, “The Nuclear Regulatory Commission Cyber Security Roadmap”	ML12135A050
SECY-14-0147, “Cyber Security for Fuel Cycle Facilities”	ML14177A264 (not publicly available due to security-related information)
SRM to SECY-14-0147, “Staff Requirements – SECY-14-0147 – Cyber Security for Fuel Cycle Facilities”	ML15083A175

Throughout the development of this rulemaking, the NRC may post documents related to this action, including public comments, on the Federal rulemaking Web site at http://www.regulations.gov under Docket ID NRC-2015-0179. The Federal rulemaking Web site allows you to receive alerts when changes or additions occur in a docket folder. To subscribe: 1) navigate to the docket folder (NRC-2015-0179); 2) click the “Sign up for E-mail Alerts” link; and 3) enter your e-mail address and select how frequently you would like to receive e-mails (daily, weekly, or monthly).

List of Subjects

10 CFR part 40

Criminal penalties, Exports, Government contracts, Hazardous materials transportation, Hazardous waste, Nuclear energy, Nuclear materials, Penalties, Reporting and recordkeeping requirements, Source material, Uranium, Whistleblowing.

10 CFR part 70

Classified information, Criminal penalties, Emergency medical services, Hazardous materials transportation, Material control and accounting, Nuclear energy, Nuclear materials, Packaging and containers, Penalties, Radiation protection, Reporting and recordkeeping requirements, Scientific equipment, Security measures, Special nuclear material,

Whistleblowing.

10 CFR part 73

Criminal penalties, Exports, Hazardous materials transportation, Incorporation by reference, Imports, Nuclear energy, Nuclear materials, Nuclear power plants and reactors, Penalties, Reporting and recordkeeping requirements, Security measures.

For the reasons set out in the preamble and under the authority of the Atomic Energy Act of 1954, as amended; the Energy Reorganization Act of 1974, as amended; and 5 U.S.C. 552 and 553, the NRC is proposing to adopt the following amendments to 10 CFR parts 40, 70, and 73.

PART 40 - DOMESTIC LICENSING OF SOURCE MATERIAL

1. The authority citation for part 40 continues to read as follows:

Authority: Atomic Energy Act of 1954, secs. 62, 63, 64, 65, 69, 81, 83, 84, 122, 161, 181, 182, 183, 184, 186, 187, 193, 223, 234, 274, 275 (42 U.S.C. 2092, 2093, 2094, 2095, 2099, 2111, 2113, 2114, 2152, 2201, 2231, 2232, 2233, 2234, 2236, 2237, 2243, 2273, 2282, 2021, 2022); Energy Reorganization Act of 1974, secs. 201, 202, 206, 211 (42 U.S.C. 5841, 5842, 5846, 5851); Uranium Mill Tailings Radiation Control Act of 1978, sec. 104 (42 U.S.C. 7914); 44 U.S.C. 3504 note.

2. In § 40.4, add a definition to read as follows:

§ 40.4 Definitions.

* * * * *

Uranium hexafluoride conversion or deconversion facility means a facility whose

principal activities are for the production, conversion, or deconversion of uranium hexafluoride.

* * * * *

3. In § 40.31, add paragraph (n) to read as follows:

§ 40.31 License applications.

* * * * *

(n) An application for a license to possess and use source material at a uranium hexafluoride conversion or deconversion facility must include a cyber security plan that demonstrates how the applicant plans to meet the requirements of § 73.53 of this chapter.

4. In § 40.35, add paragraph (g) to read as follows:

§ 40.35 Conditions of specific licenses issued pursuant to § 40.34.

* * * * *

(g) The licensee may not make a change that would decrease the effectiveness of the cyber security plan prepared pursuant to § 40.31(n) and § 73.53 of this chapter without the prior approval of the Commission. A licensee desiring to make such a change must submit an application for amendment of its license pursuant to § 40.44. The licensee may make changes to the cyber security plan without prior Commission approval if these changes do not decrease the effectiveness of the plan. The licensee must retain a copy of the cyber security plan in accordance with § 73.53 of this chapter and maintain records of changes to the plan made without prior Commission approval for 3 years from the effective date of the change, and must, within 2 months after the change is made, submit a report containing a description of each change using an appropriate method listed in § 40.5(a); and a copy of the report must be sent to the appropriate NRC Office shown in appendix A to part 73 of this chapter.

PART 70 - DOMESTIC LICENSING OF SPECIAL NUCLEAR MATERIAL

5. The authority citation for part 70 continues to read as follows:

Authority: Atomic Energy Act of 1954, secs. 51, 53, 57(d), 108, 122, 161, 182, 183, 184, 186, 187, 193, 223, 234, 274, 1701 (42 U.S.C. 2071, 2073, 2077(d), 2138, 2152, 2201, 2232, 2233, 2234, 2236, 2237, 2243, 2273, 2282, 2021, 2297f); Energy Reorganization Act of 1974, secs. 201, 202, 206, 211 (42 U.S.C. 5841, 5842, 5846, 5851); Nuclear Waste Policy Act of 1982, secs. 135, 141 (42 U.S.C. 10155, 10161); 44 U.S.C. 3504 note.

6. In § 70.22, add paragraph (o) to read as follows:

§ 70.22 Contents of application.

* * * * *

(o) Each application for a license to possess greater than a critical mass of special nuclear material 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 special nuclear material, or any other fuel cycle facility activity that the Commission determines could significantly affect public health and safety, must include a cyber security plan that demonstrates how the applicant plans to meet the requirements of § 73.53 of this chapter. A cyber security plan is not required for decommissioning activities performed pursuant to other applicable Commission regulations, including §§ 70.25 and 70.38.

7. In § 70.32, add paragraph (f) to read as follows:

§ 70.32 Conditions of licenses.

* * * * *

(f) The licensee may not make a change that would decrease the effectiveness of the

cyber security plan prepared under § 70.22(o) and § 73.53 of this chapter without the prior approval of the Commission. A licensee desiring to make such a change must submit an application for amendment of its license pursuant to § 70.34. The licensee may make changes to the cyber security plan without prior Commission approval if these changes do not decrease the effectiveness of the plan. The licensee must retain a copy of the cyber security plan in accordance with § 73.53 of this chapter and maintain records of changes to the plan made without prior Commission approval for 3 years from the effective date of the change, and must, within 2 months after the change is made, submit a report containing a description of each change using an appropriate method listed in § 70.5(a); and a copy of the report must be sent to the appropriate NRC Office shown in appendix A to part 73 of this chapter.

* * * * *

PART 73 - PHYSICAL PROTECTION OF PLANTS AND MATERIALS

8. The authority citation for part 73 continues to read as follows:

Authority: Atomic Energy Act of 1954, secs. 53, 147, 149, 161, 170D, 170E, 170H, 170I, 223, 229, 234, 1701 (42 U.S.C. 2073, 2167, 2169, 2201, 2210d, 2210e, 2210h, 2210i, 2273, 2278a, 2282, 2297f); Energy Reorganization Act of 1974, secs. 201, 202 (42 U.S.C. 5841, 5842); Nuclear Waste Policy Act of 1982, secs. 135, 141 (42 U.S.C. 10155, 10161); 44

U.S.C. 3504 note. Section 73.37(b)(2) also issued under Sec. 301, Public Law 96-295, 94 Stat. 789 (42 U.S.C. 5841 note).

9. In § 73.8, revise paragraph (b) to read as follows:

§ 73.8 Information collection requirements: OMB approval.

***** ***** ***** ***** *****

(b) The approved information collection requirements contained in this part appear in §§ 73.5, 73.20, 73.21, 73.23, 73.24, 73.25, 73.26, 73.27, 73.37, 73.38, 73.40, 73.45, 73.46, 73.50, 73.51, 73.53, 73.54, 73.55, 73.56, 73.57, 73.58, 73.60, 73.67, 73.70, 73.71, 73.72, 73.73, 73.74, and appendices B, C, and G to this part.

* * * * *

10. In § 73.46, revise paragraph (g)(6) to read as follows:

§ 73.46 Fixed site physical protection systems, subsystems, components, and procedures.

* * * * *

(g) * * *

(6) The security and cyber security programs must be reviewed at least every 12 months by individuals independent of security program management, cyber security program management, and personnel who have direct responsibility for implementation of the security and cyber security programs. The security program review must include an audit of security procedures and practices, an evaluation of the effectiveness of the physical protection system, an audit of the physical protection system testing and maintenance program, and an audit of commitments established for response by local law enforcement authorities. The cyber security program review must include an evaluation of the effectiveness of applicable cyber security controls, alternate means of protection, defensive architecture, and relevant implementing procedures for the digital assets identified through § 73.53(d)(3). The results and recommendations of the security and cyber security program reviews, and any actions taken, must be documented in a report to the licensee's plant manager and to corporate management at least one level higher than that having responsibility for the day-to-day plant operations.

These reports must be maintained in an auditable form, available for inspection for a period of 3 years.

* * * * *

11. Add § 73.53 to read as follows:

§ 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 § 70.60 of this chapter and each applicant or licensee subject to the requirements of part 40 of this chapter for the possession or use of source material at a uranium hexafluoride conversion or deconversion facility. By the later of **[DATE THAT IS 180 DAYS AFTER THE DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**, or 180 days before the anticipated date for possessing licensed material, 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 for a license to the Commission prior to the effective date of this rule, 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 to detect, protect against, and respond to a cyber attack capable of causing a consequence of concern as specified 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 § 74.51(a) of this chapter.

(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 § 74.41(a) of this chapter.

(3) *Active consequences of concern – safety.* One or more of the following that directly results from a cyber attack:

(i) A radiological exposure of 0.25 Sv (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 0.25 Sv (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; 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 specified in paragraph (c) of this section.

(3) Identify digital assets that if compromised by a cyber attack, would result in a consequence of concern specified 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 the 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 consequences of concern associated with the vital digital asset; and

(ii) Establishing and maintaining the implementing procedures that document 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 temporary compensatory measures to meet the cyber security program performance objectives. When implemented, temporary compensatory measures must be documented and tracked to completion.

(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 will be 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 for 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 do not need to be submitted for Commission review and approval, but must be documented and made available upon Commission request.

(3) The licensee may not make a change that would decrease the effectiveness of the cyber security plan without the prior approval of the Commission. A licensee desiring to make such a change must submit an application for amendment of its license.

(f) *Configuration management.* The licensee must utilize a configuration management system to ensure that changes to the facility are evaluated prior to implementation and do not adversely impact the licensee's ability to meet the cyber security program performance objectives specified in paragraph (b) of this section. This system must be documented in written procedures.

(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 of the cyber security program including, but not limited to, applicable cyber security controls, alternate means of protection, defensive architecture, and relevant implementing procedures 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, 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 (c)(2)(ii) of this section.

(3) The records required by paragraph (h)(2) of this section need not be reported to the

NRC Operations Center, but must be documented and made available upon Commission request.

(i) *Records.* The licensee must retain the cyber security plan and 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 the cyber security plan, records, reports, and documents for at least 3 years after they are superseded, unless otherwise specified by the Commission.

Dated at Rockville, Maryland, this _____ day of _____, 2017.

For the Nuclear Regulatory Commission.

Annette L. Vietti-Cook,
Secretary of the Commission.