POLICY ISSUE
(Notation Vote)

October 4, 2017 SECY-17-0100

FOR: The Commissioners

FROM: Victor M. McCree
Executive Director for Operations

SUBJECT: SECURITY BASELINE INSPECTION PROGRAM ASSESSMENT RESULTS AND RECOMMENDATIONS FOR PROGRAM EFFICIENCIES

PURPOSE:

This paper provides the results of the staff's assessment of the security baseline inspection program, including force-on-force (FOF) along with options and recommendations for Commission approval in response to the Commission's direction in Staff Requirements Memorandum (SRM) - SECY-16-0073, "Options and Recommendations for the Force-on-Force Inspection Program in Response to SRM-SECY-14-0088," dated October 5, 2016 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML16279A345). Although the U.S. Nuclear Regulatory Commission (NRC) conducts security baseline inspections, including FOF exercises, for all licensees for which a design-basis threat (DBT) applies (i.e., operating nuclear power reactors and Category I fuel cycle facilities), the focus of this paper is on security baseline inspections at nuclear power reactors.

SUMMARY:

The staff completed an assessment of the security baseline inspection program, including FOF, and has found that the overall program remains effective. The staff has identified potential efficiencies and improvements that can be applied throughout the program. Consistent with the direction in SRM-SECY-16-0073, the staff examined: (1) the use of vulnerability assessments;

CONTACT: Marissa Bailey, NSIR/DSO
301-287-3778

(2) whether crediting operator actions, the use of diverse and flexible mitigation capabilities (FLEX) equipment, or response by local, State, and Federal law enforcement would improve the realism of FOF exercises; and (3) next steps for the existing integrated response program.

While industry's efforts to provide generic guidance on the use of vulnerability assessments are on hold, the staff continues to evaluate the available assessment tools and their potential applications to security at NRC-licensed facilities. The NRC currently provides credit for a limited number of operator actions and FLEX equipment as described in Regulatory Guide (RG) 5.81.[1] The staff is evaluating the technical basis to extend the RG 5.81 criteria to a broader set of operator actions and is working with stakeholders to update the document. The staff has evaluated whether the NRC should provide credit for local, State, and Federal law enforcement in responding to a security event within the DBT and determined that it is appropriate to explore options for providing such credit. The staff is developing potential methodologies for providing credit and plans to submit a subsequent paper to the Commission that will discuss both credit for local, State, and Federal law enforcement in responding to a security event and recommendations for the integrated response program. This subsequent paper could address any improvements in FOF exercise realism that may stem from such credit.

The staff has identified three potential options for the Commission's consideration to improve the efficiency of the FOF inspection program: (1) maintain the current program of two NRC-conducted FOF exercises at each nuclear power reactor facility on a triennial basis; (2) revise the FOF inspection program to include one NRC-conducted FOF exercise, followed by a defense-in-depth exercise[2] if the licensee's performance on the first FOF exercise is rated effective or a second NRC-conducted FOF exercise if it is not; or (3) revise the FOF inspection program to include one NRC-conducted FOF exercise and an enhanced NRC inspection of a licensee-conducted annual FOF exercise. Each of these options maintains the current suite of baseline inspection activities conducted under the security baseline inspection program.

The staff requests that the Commission approve the staff's proposal to revise the FOF inspection program to include one NRC-conducted FOF exercise and an enhanced NRC inspection of a licensee conducted annual FOF exercise (Option 3).

BACKGROUND:

In SRM-SECY-16-0073, the Commission approved the staff's recommendation to perform an assessment of the security baseline inspection program, including FOF. The Commission directed the staff to avoid attempting a fundamental redesign of the program, but to identify those areas most likely to yield efficiencies and improvements. Additionally, the Commission directed the staff to determine as part of its evaluation whether crediting operator actions, the use of FLEX equipment, or response by local, State, and Federal law enforcement would improve the realism of FOF exercises. The Commission also directed the staff to evaluate how vulnerability assessments could be used to evaluate the effectiveness of licensee protective strategies, and to discuss the next steps for the integrated response program based on the staff's evaluation of crediting law enforcement response during a security event. The Commission also directed the staff to be mindful that the concept of "high assurance" of

[1] Regulatory Guide 5.81, "Target Set Identification and Development for Nuclear Power Reactors" (Official Use Only-Security Related Information) (OUO-SRI).

[2] A defense-in-depth exercise is a reduced scope FOF inspection that begins testing at or inside the protected area boundary in order to evaluate the internal layers of the licensee's protective strategy.

adequate protection found in security regulations is equivalent to "reasonable assurance" when it comes to determining the appropriate level of regulation.

DISCUSSION:

Throughout its assessment of the security baseline inspection program, the staff engaged both internal and external stakeholders, through public meetings and written correspondence. Each meeting consisted of a public session followed by a closed session which enabled discussion of security-related information with cleared stakeholders. A summary of stakeholder interactions in response to SRM-SECY-16-0073 has been developed and placed in ADAMS under accession number ML17223A335.[3] The following discussion is informed by the feedback received through these interactions.

Vulnerability Assessments

Some power reactor licensees have used a limited number of vulnerability assessment tools, primarily simulation software, to support their evaluations of proposed changes to their protective strategies and corresponding changes to their NRC-approved Physical Security Plans, Training and Qualification Plans, and Safeguards Contingency Plans (collectively referred to as "security plans"). At a March 2, 2017, public meeting, industry representatives indicated that, while they were previously interested in providing generic guidance on the use of vulnerability assessments, that industry effort is currently on hold due to other higher priority work. The staff is working with several vulnerability assessment tool vendors to gain knowledge and familiarity with the various types of tools, including a working knowledge of the data input parameters, limitations, concepts, and assumptions for each. Based on the staff's experience reviewing security plan changes, the staff has determined that these tools could add value in support of the evaluation of licensee protective strategies and security plan changes. The staff will continue to work with industry, as industry priorities allow, to move forward in this area.

Operator Actions, FLEX Equipment, and Crediting Law Enforcement

As described in RG 5.81, licensees may, in the development of their target sets, take credit for operator actions, including those associated with additional equipment such as FLEX equipment. To take such credit, the operator actions should meet the following six criteria: (1) sufficient time is available to implement actions; (2) environmental conditions allow access; (3) adversary interference is precluded; (4) equipment is available and ready for use; (5) approved procedures exist; and (6) training is conducted on the existing procedures under conditions similar to the scenarios assumed. If an operator action meets these criteria, the operator action is credited as an additional element of the target set. The NRC currently provides credit for a limited number of operator actions to ensure that, in designing the site's protective strategy, licensees only rely upon those operator actions for which there is reasonable assurance that the actions can be completed during an adversary attack and will be effective at preventing significant core damage or spent fuel sabotage. During FOF exercises, the NRC assumes that an operator action that is identified as a target set element will be completed. Industry is seeking to expand credit for operator actions in the development of target sets. On May 3, 2017, the Nuclear Energy Institute (NEI) submitted a white paper[4] that outlined a proposed

[3] Security Baseline Inspection Program Assessment Stakeholder Interactions in Response to SRM-SECY-16-0073 (ADAMS Accession No. ML17223A335).

[4] NEI Cover Letter "Security Event Mitigation Assessment (SEMA) White Paper" dated May 3, 2017 (ADAMS Accession No. ML17171A199); NEI Letter "Redacted Version of NEI Security Event Mitigation Assessment" dated May 25, 2017 (ADAMS Accession No. ML17173A129).

methodology to extend the RG 5.81 criteria to a broader set of operator actions. Although the staff continues to evaluate the technical basis for NEI's proposal, the staff would use the current change management process to approve any additional operator actions through a revision to RG 5.81. The staff will continue to work with industry on these concepts and will seek feedback from stakeholders on RG 5.81 at appropriate points during the revision process.

The methodology proposed by NEI would also provide credit for a tactical law enforcement response to preclude adversary interference to allow completion of a mitigation action or strategy, which could include the use of FLEX equipment. The staff believes that the approval of such an approach would first require a change to the current Commission policy that licensees are expected to defend against the DBT without external assistance. In promulgating the DBT Final Rule[5], the Commission recognized that "[t]he defense of our nation's critical infrastructure is a shared responsibility between the NRC, the [Department of Defense], the [Department of Homeland Security], Federal and State law enforcement and other Federal agencies. A reasonable approach in determining the threat requires making certain assumptions about these shared responsibilities." As further documented in the response to comments on the DBT Final Rule, "[t]he Commission has determined that the DBTs, as articulated in the rule, are based on adversary characteristics against which a private security force can reasonably be expected to defend." The Statement of Considerations (SOC) for the Power Reactor Security Requirements Final Rule[6] further states that "a licensee's ability to defend against the design basis threat of radiological sabotage is not dependent on the availability of offsite responders." Finally, the SOC for the DBT Final Rule states that "local law enforcement and other non-licensee security personnel already stationed at the owner-controlled boundary or entry portals of some licensee facilities are not part of the licensee workforce and not subject to NRC regulatory authority."

The Commission has determined that licensees are reasonably expected to defend against the DBT and licensees design their security programs to do so. It is, therefore, reasonable for the FOF exercises to evaluate the ability of the licensee's security force to defend against the DBT unassisted. The NRC has no jurisdiction over law enforcement agencies, and the NRC does not have the ability to verify their availability. However, the current policy that the licensee maintain sole responsibility for defending against the DBT does not ignore the reality of law enforcement response to a security event within the DBT. NRC regulations currently require licensees to notify law enforcement agencies as part of their response procedures, and to document agreements with law enforcement agencies, including estimated response times and capabilities, to the extent practicable.[7]

Consistent with the Commission's direction, the staff has evaluated whether the NRC should provide credit for local, State, and Federal law enforcement in responding to a security event beyond the DBT. Because of the potential benefits from licensee coordination with law enforcement agencies, including law enforcement tactical teams, the staff has determined that it is appropriate to explore options for providing such credit. The staff plans to continue stakeholder engagement on this topic and to develop potential methodologies to provide credit for local, State, and Federal law enforcement response. The staff is considering several possible approaches to providing credit for local, State, and Federal law enforcement response, including an approach proposed by industry; establishing a new process for determining site-specific bounding times after which it could be assumed that law enforcement can support the response; and/or creating a regulatory framework for integrated response. Because these

---

[5] Design Basis Threat Final Rule, March 19, 2007, 72 FR 12705.
[6] Power Reactor Security Requirements Final Rule, March 27, 2009, 74 FR 13940.
[7] See Title 10 of the *Code of Federal Regulations* (10 CFR) 73.55(k)(8)(iii), (k)(9).

approaches would represent a change to Commission policy, the staff plans to provide the results of its evaluation, along with options and recommendations, in a subsequent paper to the Commission.

In responding to the Commission's direction to provide next steps for the integrated response program, the staff reviewed the efforts that the NRC, with the support of other Federal agencies, has conducted over the past 10 years to establish a voluntary integrated response program. The staff found that because industry has not fully supported this effort, the program has not achieved its full potential. Consistent with the discussion in COMSECY-13-0005,[8] the staff plans to propose an option in the subsequent paper to the Commission related to whether rulemaking is needed to ensure full implementation by industry of the elements of the integrated response program.

Security Baseline Inspection Program Assessment

The staff assessed the security baseline inspection program in two phases. In the initial phase, the staff reviewed current staff activities and compiled both internal and external stakeholder input to identify areas likely to yield improvements and efficiencies. Based on the results of the initial phase of the assessment, the staff identified focus areas for a review of all security baseline inspection program procedures. The staff developed a charter[9] to provide guidance and direction for an inspection procedure (IP) review team, composed of security inspectors and team leaders from headquarters and each regional office, to carry out the second phase of the assessment. The staff presented the objectives and focus areas for the IP review team during a public meeting on March 2, 2017, and obtained feedback from internal and external stakeholders.

In the second phase, the IP review team reviewed all of the security baseline inspection program procedures. The review focused on: (1) identifying redundancies; (2) identifying opportunities to streamline the inspection process; and (3) verifying that the IPs are consistent with the Commission direction on the concept of "high assurance." In so doing, the team considered specific recommendations provided by NEI in its January 26, 2017[10], letter. The team developed a summary of its recommendations.[11] In its summary, the team identified several opportunities to eliminate redundant IP sample items and identified potential opportunities for increased inspection efficiency. The team also recommended revising the periodicity of one IP and recommended revisions to Inspection Manual Chapter 0609, Appendix E, "Security Significance Determination Process for Power Reactors."

As part of its IP review, the staff has identified specific changes to the FOF inspection process. The staff coordinated with both internal and external stakeholders, and identified several potential process improvements and efficiencies. For example, an extra week could be added between the planning and exercise portions of the FOF inspection; this would permit licensees and staff more time to prepare documentation for the exercises. Also, the Composite Adversary

---

[8] COMSECY-13-0005, "Integrated Law Enforcement Response at Nuclear Power Plants" dated February 7, 2013 (ADAMS Accession No. ML12305A419) (OUO-SRI).

[9] "Charter for the Security Baseline Inspection Program Assessment and Efficiency Review in Response to SRM-SECY-16-0073" dated February 28, 2017 (ADAMS Accession No. ML17144A256) (OUO-SRI).

[10] NEI Letter to B. Holian, "Industry Recommendations Related to Memorandum, 'Staff Requirements – SECY-16-0073 – Options and Recommendations for the Force-on-Force Inspection Program in Response to SRM-SECY-14-0088,'" dated January 26, 2017 (ADAMS Accession No. ML17046A218).

[11] Summary of Security Inspection Procedure Review Team Recommendations dated August 21, 2017 (ADAMS Accession No. ML17191A402) (OUO-SRI).

Force (CAF) Director could join the NRC inspection team's planning week activities to streamline the scenario development process. Finally, the CAF team could arrive on-site 1 week earlier to allow training for the exercise week during normal work hours and minimize after-hours or weekend sessions.

The staff has a separate, ongoing initiative to review and update the security baseline inspection program significant determination processes (SDPs). The staff will incorporate the IP review team recommendations and ensure that the SDPs reflect both the concept of "high assurance" of adequate protection as described in SRM-SECY-16-0073, and an appropriate level of risk-informed decision-making when assessing findings. The staff is moving forward with revisions to the IPs and the associated SDPs using the current change management process. The staff would seek Commission approval or provide notification to the Commission (as appropriate per the Commission's direction in SRM-COMSECY-16-0022[12]) of any new or revised SDPs or IPs.

Force-on-Force Inspection Options

Section 170D of the Atomic Energy Act of 1954, as amended (AEA), requires that the NRC conduct security evaluations at licensed facilities, as the Commission considers to be appropriate, at least once every 3 years. These security evaluations are to assess the ability of the licensee's security force to defend against the applicable DBT. The AEA further requires that the security evaluations include FOF exercises (the number of exercises is not specified); that the exercises simulate security threats in accordance with the DBT to the maximum extent practicable; and that the Commission mitigate any potential conflict of interest that could influence the result of an exercise, as the Commission determines to be necessary and appropriate. Consistent with these requirements, each of the options set forth below would include at least one NRC-conducted FOF exercise during the NRC's triennial security evaluation of each nuclear power reactor licensee and maintains the NRC's role in conducting security evaluations at licensed facilities.

Based on its assessment of the security baseline inspection program, the staff has found that the program, including FOF, is effective. The staff has, however, identified potential efficiencies and improvements. As discussed above, the staff has assessed that revising the IPs and SDPs in the security baseline inspection program will result in some process improvements and efficiency gains for both the program as a whole and FOF exercises, specifically. In addition, the staff has identified an opportunity to adjust the FOF inspection portion of the program to realize additional improvements and efficiencies. Conceptual models of each of these options, including a more detailed discussion of their advantages and disadvantages, are provided in Enclosure 1. The staff would work with industry to identify the lead plants for implementing options 2 or 3, if approved by the Commission.

FOF Option 1 – Implement process improvements and maintain the current program of two NRC-conducted FOF exercises at each nuclear power reactor facility on a triennial basis

Option 1 represents the current FOF inspection program, with implementation of the process improvements discussed in the previous section. This option consists of a planning week, during which the NRC would plan two FOF exercises, and an exercise week, during which the NRC would evaluate licensee performance during the two exercises. The inspection program

[12] SRM-COMSECY-16-0022, "Proposed Criteria for Reactor Oversight Process Changes Requiring Commission Approval and Notification", dated May 12, 2017 (ADAMS Accession No. ML17132A359).

would continue under the currently established framework using IP 71130.03, "Contingency Response – Force-on-Force Testing," and the current SDP, pending any revisions based on the SDP working group. The current FOF SDP uses the two NRC-conducted exercise results as inputs to assess overall licensee performance during FOF inspections.

The advantages of this option are that it provides the most program stability while implementing the IP review team recommendations, pursuing revisions to the SDP, and monitoring licensee performance during a period of resource reductions for both the NRC and industry. The disadvantages of this option are that it provides the smallest resource savings for both the NRC and industry and it does not take advantage of the opportunity to gain additional insights from assessing one FOF exercise from a different perspective (i.e., evaluation of defense-in-depth exercise or enhanced inspection of licensee-conducted exercises).

FOF Option 2 – Revise the FOF inspection program to include one NRC-conducted FOF exercise, followed by a defense-in-depth exercise if the licensee's performance on the first FOF exercise is rated effective or a second NRC-conducted FOF exercise if it is not

Option 2 is a modification of the current inspection program and incorporates aspects of NEI's defense-in-depth proposal outlined in attachment 3 to its January 26, 2017, letter. This option would maintain both the current planning and exercise weeks, modified as discussed in Option 1; however, the NRC inspection team would include a placeholder in the plan for the second exercise from which a defense-in-depth exercise would begin. During the exercise week, if the licensee's performance in the initial exercise was evaluated as effective, the NRC would evaluate a defense-in-depth exercise instead of the second, full-scope FOF exercise. This exercise would consist of a CAF team complement, which would begin testing the licensee's defenses at or within the protected area boundary at a pre-determined location. This would allow the NRC to reduce the scope of the exercise and focus the inspection on the internal layers of the licensee's protective strategy. If the initial FOF exercise was evaluated as marginal, indeterminate, or ineffective, the inspection team would conduct a second NRC-conducted FOF exercise rather than a defense-in-depth exercise.

The advantages of this option are that it would provide an opportunity for the NRC to perform a specific evaluation of a licensee's internal protective strategy. Also, for licensees that have an effective first FOF exercise, there may be greater resource savings, as outlined in Enclosure 1, for both the NRC and the licensee than those associated with option 1 because the defense-in-depth exercise would be designed to be shorter and would include fewer players. The primary disadvantage of this option is the risk of unintended consequences. By focusing on the internal strategy in the second exercise, the NRC may unintentionally encourage licensees with an effective external strategy to divert resources from maintaining that effective strategy to make unnecessary changes to their internal strategy solely for the purpose of performing well in the defense-in-depth exercise. Furthermore, this option would require resources to plan, coordinate, and carry out a second NRC-conducted FOF exercise even though it would not be needed if the first exercise is effective. Although NEI initially proposed the defense-in-depth exercise concept, NEI stated in a July 17, 2017, letter that it did not prefer this option.[13]

FOF Option 3 – Revise the FOF inspection program to include one NRC-conducted FOF exercise and an enhanced NRC inspection of a licensee-conducted annual FOF exercise

[13] NEI letter to Marissa Bailey dated July 17, 2017, "Updated Industry Input on Options Being Considered for Force-on-Force Exercise Inspections" (ADAMS Accession No. ML17198B306).

Option 3 would maintain one NRC-conducted FOF exercise, modified as discussed in Option 1, and would include an enhanced NRC inspection and evaluation of a licensee-planned and conducted FOF exercise. Licensees currently conduct annual exercises for each security shift as part of the performance evaluation program required by Title 10 of the *Code of Federal Regulations* Part 73 Appendix B. The NRC's current inspection procedure for these licensee-conducted annual exercises focuses on an evaluation of the licensee's implementation of the training and qualification elements of its performance evaluation program, not the effectiveness of its protective strategy. Under this option, the NRC would conduct an enhanced inspection of a regularly scheduled licensee-conducted annual FOF exercise. Key differences between the NRC-conducted exercise and the licensee-conducted exercise include that the licensee would develop the exercise scenario, and the adversary force would be composed of licensee personnel. In addition to evaluating the performance of the licensee security force, the enhanced NRC inspection of the licensee-conducted exercise would review and evaluate the performance of the adversary force and the development and implementation of the exercise scenario.

The staff identified several advantages of this option. The NRC would be able to shorten both the FOF planning and exercise weeks because the NRC would plan and evaluate one exercise. Additionally, as with option 2, this option would provide staff with a different perspective through which to observe and evaluate the licensee's implementation of its protective strategy. Conducting an enhanced evaluation of a licensee-conducted FOF exercise would allow the NRC to better assess licensees' understanding of the tactics, techniques, and procedures that might be used by real world adversaries. Additionally improved licensee performance in the development and conduct of their annual exercises could facilitate licensees' self-assessment and identification of security issues to the benefit of their overall security programs.

Finally, this option would provide the staff with data that would inform a thorough consideration of potential future program changes, such as NEI's proposal to "ultimately [allow] licensees to prepare and conduct FOF exercises as a replacement for the NRC-conducted FOF exercises."[14] Specifically, the staff would be able to assess whether licensee-conducted FOF exercises can mitigate conflicts of interest and realistically represent the DBT sufficient to meet the requirements of Section 170D of the AEA. Additionally, in SRM-SECY-16-0073 the Commission directed that, prior to any staff assessment of an industry proposal that the NRC observe and evaluate licensee-conducted FOF exercises rather than the NRC conducting FOF exercises, the Office of General Counsel complete a legal analysis on this matter. That legal analysis was provided to the staff and the Commission in February 2017, and is non-publicly available because it contains Official Use Only – Attorney/Client Privileged Information.

As noted in NEI's letter of July 17, 2017, Option 3 is the industry's preferred option. The staff identified some disadvantages for this option. Initially, this option could increase complexities with the scheduling process due to the need to avoid conflicts among multiple NRC inspections and licensee operations, and increase staff travel costs to inspect the licensee-conducted exercise. The continued use of the Reactor Programs System to coordinate inspection planning would help mitigate the scheduling issue and the reduction in resources achieved by eliminating the second NRC-conducted FOF exercise would help offset the travel costs associated with inspecting the licensee-conducted exercises. Further, consistent with the discussion in SECY-03-0208, the use of a licensee adversary force is subject to perceptions of conflict of

[14] Id.

interest; however, the staff expects that any potential conflict would be mitigated by the NRC's independent evaluation of the licensee-conducted exercise.[15]

In summary, Option 3 would increase the efficiency of the FOF inspection program and allows the staff to evaluate the licensee's performance in a new manner without compromising the NRC's regulatory oversight responsibility.

COMMITMENT:

As discussed above, the staff has evaluated whether the NRC should provide credit for local, State, and Federal law enforcement in responding to a security event within the DBT and found that this would be a change in Commission policy. The staff is developing potential methodologies for providing credit and plans to submit a subsequent paper to the Commission that will discuss both credit for local, State, and Federal law enforcement in responding to a security event and recommendations for the integrated response program. This subsequent paper could address any improvements in FOF exercise realism that may stem from such credit.

RECOMMENDATIONS:

The NRC staff recommends that the Commission approve the staff's proposal to modify the FOF inspection program to include one NRC-conducted FOF exercise and an enhanced NRC inspection of a licensee-conducted annual FOF exercise (Option 3).

RESOURCES:

Resource needs for fiscal year (FY) 2018 and FY 2019 are included in the FY 2018 Current Estimate and FY 2019 Budget Request. Resources for FY 2020 and beyond will be addressed through the Planning, Budgeting, and Performance Management process.

COORDINATION:

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

/RA/

Victor M. McCree
Executive Director
for Operations

Enclosure:
As stated

[15] SECY-03-0208, "Adversary for Force-on-Force Exercises at NRC-Licensed Facilities", dated December 3, 2003 (ADAMS Accession No. ML051020052).

SUBJECT: SECURITY BASELINE INSPECTION PROGRAM ASSESSMENT RESULTS AND RECOMMENDATIONS FOR PROGRAM EFFICIENCIES DATED: OCTOBER 4, 2017.

SRM-S16-0073-1 & 3
ADAMS ACCESSION Nos.: Pkg: ML17240A360; SECY: ML17223A279;

OFFICE	NSIR/DSO	NSIR/DSO	NSIR/DPCP	NRR	NMSS
NAME	TKeene	MBailey	JAndersen	BHolian	MDapas (SMoore for)
DATE	08/10/2017	08/18/2017	08/17/2017	08/31/2017	09/07/2017
OFFICE	OCFO	Region I	Region II	Region III	Region IV
NAME	MWylie	DDorman	CHaney (LDudes for)	CPederson	KKennedy
DATE	09/06/2017	08/25/2017	09/06/2017	09/14/2017	09/06/2017
OFFICE	OE	OGC	NSIR Mailroom Tech Edit	NSIR	EDO
NAME	PHolahan (PPeduzzi for)	JMaltese	CRaynor	SWest	V. McCree
DATE	08/25/2017	09/21/2017	09/21/2017	9/25/2017	10/4/17

U.S. Nuclear Regulatory Commission Staff Response to SRM-SECY-16-0073
Detailed Description of Force-on-Force Inspection Program Options

Although the U.S. Nuclear Regulatory Commission (NRC) conducts security baseline inspections, including force-on-force (FOF) exercises, for all licensees for which a design-basis threat (DBT) applies (i.e., operating nuclear power reactors and Category I fuel cycle facilities), the focus of this enclosure is on security baseline inspections at nuclear power reactors.

Background

The fundamental building blocks that form the framework for the reactor oversight process (ROP) for nuclear power reactors are the seven cornerstones: initiating events; mitigating systems; barrier integrity; emergency preparedness; occupational radiation safety; public radiation safety; and security. This ROP framework is based on the principle that the NRC's mission of assuring public health and safety and promoting common defense and security is met when the agency has reasonable assurance that licensees are meeting the objectives of the six cornerstones of safety and the security cornerstone.

The security baseline inspection program is designed to gather information to determine whether a licensee is meeting the objective of the security cornerstone. Specifically, the objective of the security cornerstone is to provide assurance that a power reactor licensee's security system and material control and accounting program meet the applicable general performance objectives and requirements of Title 10 of the *Code of Federal Regulations* (10 CFR) Part 73, "Physical Protection of Plants and Materials," and 10 CFR Part 74, "Material Control and Accounting of Special Nuclear Material."

Overall, the security baseline inspection program emphasizes achieving a balanced review of a cross section of licensee activities important to the security of the facility, with inspection resources assigned to each area based on its relative importance to meeting the objectives of the security cornerstone. The security baseline inspection program provides the minimum examination of the facilities, licensee activities, and licensee programs and procedures to determine whether licensees are meeting applicable regulatory requirements. The inspection program incorporates several baseline inspections and a performance-based FOF inspection to assess the licensee's ability to implement its strategy for protecting against the DBT. As discussed in Inspection Manual Chapter (IMC) 2201[1], the inspection frequency and sample size for each inspectable area are based on risk information and security insights, and are designed to identify problems before a licensee's performance deteriorates to unacceptable levels.

The security baseline inspection program's inspectable area periodicity, and annualized estimated resources for nuclear power reactors are shown in Table 1 below.

[1] IMC 2201, "Security Inspection Program for Operating Commercial Nuclear Power Reactors" (Official Use Only-Security Related Information) (OUO-SRI) (Agencywide Documents Access and Management System (ADAMS) Accession No. ML13234A497).

Physical Security Baseline Inspection Procedures (IP) and Estimated Resources[2]
(Table 1)

Inspection Procedure No.	Title	Frequency	Annualized Estimated Resources[3]
71130.01	Access Authorization	Triennial	8
71130.02	Access Control	Annual	27
71130.03	Contingency Response - Force-on-Force Testing	Triennial	131
71130.04	Equipment Performance, Testing and Maintenance	Biennial	18
71130.05	Protective Strategy Evaluation	Triennial	30
71130.06	Protection of Safeguards Information	Triennial	2
71130.07	Security Training	Biennial	14
71130.08	Fitness-For-Duty Program	Triennial	8
71130.11	Material Control and Accounting	Triennial	4
71130.14	Review of Power Reactor Target Sets	Triennial	3

Under the Protective Strategy Evaluation and Performance Evaluation Program (IP 71130.05) portion of the security baseline inspection program, the NRC conducts an inspection of the licensee's protective strategy and an assessment of the fundamental components of the licensee's performance evaluation program, which includes training and self-assessment through required, periodic drills and exercises. The intent of this IP is not to assess the outcome of an FOF exercise but, rather, to evaluate the licensee's implementation of processes and procedures to achieve its intended training objectives, consistent with Section VI, paragraph C.3, of Appendix B to 10 CFR Part 73. The Contingency Response – Force-on-Force Testing (IP 71130.03) portion of the security baseline inspection program is the only performance-based assessment of licensees' protective strategies and how licensees integrate and implement the components of their security programs to protect against the DBT.

The staff has implemented several changes to the FOF inspection program over the past four triennial inspection cycles (each inspection cycle is 3 years in duration). During the first triennial inspection cycle (2004-2007), each FOF inspection consisted of three FOF exercises. Since that first cycle, the program has matured and been updated through the ROP self-assessment processes and based on input from stakeholders. In 2014, the staff revised the FOF inspection program to reduce the number of FOF exercises from three to two, expand the formal FOF exercise critique process, and implement compliance-based inspection of licensee-conducted annual FOF exercises during the region-led Protective Strategy Evaluation and Performance Evaluation Program evaluation. Since 2014, the staff has implemented several additional

[2] Id.
[3] Direct inspection effort (hours), based on conducting the nominal range of inspection requirements within the inspectable area.

changes to the program, primarily in response to the lessons-learned review described in SECY-14-0088,[4] which have resulted in a reduction to the average number of direct inspection effort (DIE) hours for the FOF inspection by approximately 17 percent to 360[5] DIE hours per inspection. Based on its assessment of the security baseline inspection program, the staff has found that the program, including FOF, is effective. The staff has, however, identified potential efficiencies and improvements.

The staff engaged with stakeholders during public and closed meetings throughout the assessment process. A summary of the stakeholder interactions in response to Staff Requirements Memorandum (SRM) for SECY-16-0073[6] is included in ADAMS under accession number ML17223A335[7]. Resource savings noted in the discussion below are based on estimated reductions in on-site inspection time. Due to the modest nature of the estimated resource savings, this was not a critical factor in the staff's final recommendation. The staff requested industry representatives and the Nuclear Energy Institute (NEI) to provide quantitative resource impacts of the proposed options; these stakeholders did not provide the information, so the staff assessment of resource implications is based on the staff's experience and observations during the conduct of FOF exercises throughout the previous inspection cycles.

Force-on-Force Inspection Procedure Options

In SRM-SECY-16-0073, the Commission directed the NRC staff to conduct an assessment of the security baseline inspection program, including the FOF program. In response to the Commission's direction, the NRC staff developed three options for potential revisions to the FOF inspection program.

The staff has assessed that the security baseline inspection program effectively evaluates licensees' security programs and meets the agency's goals of ensuring safety and security through objective risk-informed inspections; however, the staff has identified opportunities to improve the efficiency of the inspection program. The staff's proposal to implement changes to the FOF inspection program is based on maintaining the other security baseline inspections during the triennial inspection period to maintain an appropriate level of regulatory stability and oversight in order to readily identify any potential degradation in licensees' security programs.

As part of the security baseline inspection procedure assessment, the staff completed a review of the governing IMC and associated IPs. The staff established a working group composed of regional and headquarters security inspectors. The working group identified and recommended correction of redundant inspection sample items and IP inefficiencies. The detailed list of recommendations, provided in the working group summary,[8] are being pursued by the staff and could be implemented regardless of which option the Commission approves.

---

[4] SECY-14-0088, "Proposed Options to Address Lessons-Learned Review of the U.S. Nuclear Regulatory Commission's Force-on-Force Inspection Program in Response to Staff Requirements Memorandum – COMGEA/COMWCO-14-0001" dated August 20, 2017(ADAMS Accession No. ML14139A231).

[5] The previous IP allocation for FOF was 435 hours of DIE. The current IP allocation for FOF is 393 hours of DIE; however, recently implemented efficiencies have not yet been incorporated into the IP allocation.

[6] SRM-SECY-16-0073, "Options and Recommendations for the Force-on-Force Inspection Program in Response to SRM-SECY-14-0088," dated October 5, 2016 (ADAMS Accession No. ML16126A140).

[7] "Security Baseline Inspection Program Assessment Stakeholder Interactions in Response to SRM-SECY-16-0073" (ADAMS Accession No. ML17223A335).

[8] Security Baseline Inspection Procedure Review Team Recommendations dated August 21, 2017 (ADAMS Accession No. ML17191A402) (OUO-SRI).

During the assessment process, the staff identified some proposed enhancements/efficiencies which, in addition to the staff recommendations noted in the previous paragraph, apply to all options and can be pursued and incorporated into the FOF inspection process to minimize NRC on-site time:

1. Add an extra week between the planning and exercise portions of the FOF inspection to permit licensees and staff more time to prepare documentation for the exercises.
2. Embed the Composite Adversary Force (CAF) director with NRC staff during the planning week activities to streamline the scenario development process.
3. The CAF Team could arrive on-site 1 week earlier to allow training for the exercise week during normal work hours and minimize after-hours/weekend sessions.

The discussion of the FOF significance determination process (SDP) for each option below is based on the current FOF SDP. The staff has a separate, ongoing initiative to review and update the security baseline inspection program SDPs. The working group recommendations have been provided to the SDP task force and the staff is moving forward with revisions to the IPs and the associated SDPs using the current change management process. The staff would seek Commission approval or provide notification to the Commission (as appropriate per the Commission's direction in SRM-COMSECY-16-0022[9]) of any new or revised SDPs or IPs.

FOF Option 1 – Implement process improvements and maintain the current program of two NRC-conducted FOF exercises at each nuclear power reactor facility on a triennial basis

This option represents the current FOF inspection program, with the implementation of the process improvements discussed above. This option consists of an A-week, during which the NRC would plan two FOF exercises, and a B-week, during which the NRC would evaluate licensee performance during the conduct of the two NRC-planned exercises. The inspection program would continue under the currently established framework using IP 71130.03, and the current FOF SDP, pending any revisions based on the SDP task force. The current FOF SDP uses the two NRC-planned exercise results as inputs to assess overall licensee performance during FOF inspections.

The advantages of this option are that it provides the most program stability while implementing the IP review team recommendations, pursuing revisions to the FOF SDP, and monitoring licensee performance during a period of resource reductions for both the NRC and industry.

The disadvantages of this option are that it provides the smallest resource savings for both the NRC and industry and it does not take advantage of the opportunity to gain additional insights from assessing one FOF exercise from a different perspective.

As noted in Table 2, this option is estimated to result in a reduction in 16 hours per inspection of on-site time through the CAF team efficiencies and streamlined procedures. This option is estimated to result in minimal resource savings for licensees because it would preserve the current two-exercise process and licensee staffing requirements for the exercises would remain unchanged.

[9] SRM-COMSECY-16-0022, "Proposed Criteria for Reactor Oversight Process Changes Requiring Commission Approval and Notification" dated May 12, 2017 (ADAMS Accession No. ML17132A359).

FOF Option 2 – Revise the FOF inspection program to include one NRC-conducted FOF exercise, followed by a defense-in-depth exercise if the licensee's performance on the first FOF exercise is rated effective or a second NRC-conducted FOF exercise if it is not

This option is a modification of the current inspection program and incorporates aspects of NEI's defense-in-depth proposal outlined in attachment 3 in the January 26, 2017, letter.[10] This option would maintain both the A- and B-weeks; however, the NRC inspection team would include a placeholder in the plan for the second exercise from which a defense-in-depth exercise would begin. During B-week, if the initial NRC-planned FOF exercise outcome was marginal, indeterminate, or ineffective, the team would conduct a second NRC-conducted FOF exercise.

If the licensee's initial exercise outcome was effective, the NRC would evaluate a defense-in-depth exercise instead of the second full-scope FOF exercise. The defense-in-depth exercise would consist of a CAF team complement, which would begin testing the licensee's defenses at or within the protected area boundary at a pre-determined location. This would allow the NRC to reduce the scope of the exercise and focus the evaluation on the internal layers of the licensee's protective strategy. Since the adversary would be starting at this internal starting point, a loss of a target set would not necessarily result in a regulatory finding. The NRC would assess licensee performance via the current FOF SDP when the licensee's performance was other than effective during the initial FOF exercise. A new SDP and a new or revised IP would need to be developed for inspection and assessment of defense-in-depth exercises.

The potential advantages of this option are that it would provide an opportunity for the NRC to perform a specific evaluation of a licensee's internal protective strategy and may promote integrated use of strategies, tactics, and physical components. Also, for licensees that have an effective first FOF exercise, there may be greater resource savings for both the NRC and the licensee than those estimated under option 1.

There are also disadvantages to this option. First, there is a risk of unintended consequences if a licensee has an otherwise effective external protective strategy and makes unnecessary changes to its internal strategy to perform well in the defense-in-depth exercise. By focusing on the internal strategy in the second exercise, the NRC may unintentionally encourage licensees with an effective external strategy to divert resources from maintaining that effective strategy to make unnecessary changes to their internal strategy solely for the purpose of performing well in the defense-in-depth exercise. Furthermore, this option would require resources to plan, coordinate, and carry out a second NRC-conducted FOF exercise even though it would not be needed if the first exercise is effective. Although NEI initially proposed a defense-in-depth exercise, NEI stated in a July 17, 2017, letter that it did not prefer this option.[11]

The staff estimates that this option would reduce on-site time by approximately 28 to 36 hours per inspection, due to the reduced time required to conduct the defense-in-depth exercise when compared to a complete NRC-planned FOF exercise for a licensee that is evaluated as effective on the first exercise and subsequently completes a defense-in-depth inspection. If a licensee is required to conduct two NRC-planned exercises, the staff estimates a 12-hour reduction in time on-site. This option would also result in resource savings for licensees due to the reduced

[10] NEI letter to B. Holian, "Industry Recommendations Related to Memorandum, 'Staff Requirements – SECY-16-0073 – Options and Recommendations for the Force-on-Force Inspection Program in Response to SRM-SECY-14-0088,'" dated January 26, 2017 (ADAMS Accession No. ML17046A218).
[11] NEI letter to Marissa Bailey dated July 17, 2017, "Updated Industry Input on Options Being Considered for Force-on-Force Exercise Inspections" (ADAMS Accession No. ML17198B306).

number of exercise controllers for the limited scope exercise and due to the reduced time needed to conduct the defense-in-depth exercise.

FOF Option 3 – Revise the FOF inspection program to include one NRC-conducted FOF exercise and an enhanced NRC inspection of a licensee-conducted annual FOF exercise

Option 3 would maintain one NRC-conducted FOF exercises and would include an enhanced NRC inspection and evaluation of a licensee-planned and conducted FOF exercise. Licensees currently conduct annual exercises for each security shift as part of the performance evaluation program required by 10 CFR Part 73 Appendix B. The NRC's current inspection procedure for these licensee-conducted annual exercise focuses on an evaluation of the licensee's implementation of the training and qualification elements of its performance evaluation program, not the effectiveness of its protective strategy. Under this option, the NRC would plan and inspect one exercise and would conduct an enhanced inspection of a regularly scheduled licensee-conducted annual FOF exercise. Key differences between the NRC-conducted exercise and the licensee-conducted exercise include that the licensee would develop the exercise scenario, and the adversary force would be composed of licensee personnel. In addition to evaluating the performance of the licensee security force, the enhanced NRC inspection of the licensee-conducted exercise would review and evaluate the performance of the adversary force and the development and implementation of the exercise scenario.

This option considers the maturity and robustness of the current security baseline inspection program, and is an effort to reduce burden where possible and create efficiencies by leveraging the current regulatory oversight structure, while maintaining the NRC's ability to effectively evaluate licensee performance and preserve the integrity of the NRC's regulatory oversight.

Under this option, licensees would still be required to enter deficiencies into the corrective action program upon identification through the critique process and the current FOF IP. This option would require development of a new or revised IP and associated SDP to evaluate the licensee-conducted exercise. The new or revised IP would use performance-based criteria consistent with the current FOF IP.

The staff identified several advantages of this option. This option would provide staff with a different and additional perspective through which to observe and evaluate the licensee's implementation of its protective strategy. Conducting an enhanced evaluation of a licensee-conducted FOF exercise would allow the NRC to better assess licensees' understanding of the tactics, techniques, and procedures that might be used by real world adversaries. Improved licensee performance in the development and conduct of their annual exercises could facilitate licensees' self-assessment and identification of security issues to the benefit of their overall security programs. This option would provide the staff with data that would inform a thorough consideration of potential future program changes, such as NEI's proposal to "ultimately [allow] licensees to prepare and conduct FOF exercises as a replacement for the NRC-conducted FOF exercises."[12]

Specifically, the staff would be able to assess whether licensee-conducted FOF exercises can mitigate conflicts of interest and realistically represent the DBT sufficient to meet the requirements of Section 170D of the Atomic Energy Act of 1954, as amended. Additionally, in SRM-SECY-16-0073 the Commission directed that, prior to any staff assessment of an industry proposal that the NRC observe and evaluate licensee-conducted FOF exercises rather than the

[12] Id.

NRC conducting FOF exercises, the Office of General Counsel complete a legal analysis on this matter. That legal analysis was provided to the staff and the Commission in February 2017, and is non-publicly available because it contains Official Use Only – Attorney/Client Privileged Information. Finally, the staff has determined that this option will provide the largest reduction in DIE hours and would also provide some resource savings by only performing one NRC-conducted FOF exercise, which would shorten both the FOF planning and exercise weeks. As noted in its letter of July 17, 2017, the industry prefers this option.

However, the staff identified some disadvantages for this option. This process initially could increase complexities with the scheduling process due to the need to avoid conflicts among multiple NRC inspections and licensee operations. The continued use of the Reactor Programs System to coordinate inspection planning would mitigate this issue. Although this option would result in the largest, albeit moderate, resource reduction for both the NRC and licensees, travel expenditures, both time and cost, associated with a new or enhanced inspection could counteract some of the estimated on-site resource savings.

The staff estimates that this option would reduce on-site time by approximately 56 hours per inspection due to the reduced time required to plan and develop one FOF exercise during A-week, and the elimination of one exercise day in B-week. The estimated reduction in hours includes the NRC on-site time associated with inspecting the licensee annual exercise. Additional savings would be realized due to a reduction of the Multiple Integrated Laser Engagement System gear support through the elimination of one exercise, which would offset the increased travel costs noted above. This option is estimated to result in resource savings for licensees through the elimination of one FOF exercise and the associated staffing requirements. Further, consistent with the discussion in SECY-03-0208, the use of a licensee adversary force is subject to perceptions of conflict of interest; however, the staff expects that any potential conflict would be mitigated by the NRC's independent evaluation of the licensee-conducted exercise.[13]

Option 3 would increase the efficiency of the FOF inspection program and allow the staff to evaluate the licensee's ability to implement its protective strategy while reducing staff resources, without compromising the NRC's regulatory oversight responsibility.

The following table (Table 2) provides an overview of the estimated change to the on-site DIE for each of the three options when compared to the current FOF inspection DIE allocation. The table only reflects an evaluation of on-site DIE for the NRC staff.

[13] SECY-03-0208, "Adversary for Force-on-Force Exercises at NRC-Licensed Facilities", dated December 3, 2003 (ADAMS Accession No. ML051020052)

Contingency Response - FOF Testing (IP 71130.03) DIE
Comparison based on proposed options (Table 2)

Option	Estimated number of on-site DIE hours	Total estimated DIE hours (on-site plus in-office)	Estimated change from current program
Current FOF Inspection	320	360*	0
Option 1	304	344	-16
Option 2	284 to 292 (effective) 308 (other than effective)	324 to 332 (effective) 348 (other than effective)	-36 to -28 (effective) -12 (other than effective)
Option 3	264	304	-56

*Note, the current IP allocation is 393 hours of DIE; however, the staff has already implemented some efficiencies

Next Steps

Upon receipt of the SRM from the Commission, the staff will begin developing the new or revised IPs and SDPs, as appropriate. The staff estimates that it will require approximately 12 months to develop an inspection program based on Option 3 for the Commission's consideration per the direction in SRM-COMSECY-16-0022, and approximately 18 months for an inspection program based on Option 2. The staff would work with industry to identify the lead plants for implementing options 2 or 3, should either of these options be approved by the Commission.

POLICY ISSUE
(Notation Vote)

October 4, 2017 SECY-17-0099

FOR: The Commissioners

FROM: Victor M. McCree
Executive Director for Operations

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

PURPOSE:

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

SUMMARY:

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

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

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

establish, implement, and maintain a cyber security program designed to promote common defense and security and to provide reasonable assurance that the public health and safety remain adequately protected against the evolving risk of cyber attacks. As such, the licensee's cyber security program would enable the licensee to detect, protect against, and respond to a cyber attack capable of causing one or more of the consequences of concern defined in the proposed rule.

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

BACKGROUND:

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

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

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

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

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

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

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

DISCUSSION:

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

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

security program. Accordingly, the proposed requirements would apply to each applicant or licensee that is or plans to be authorized to: (1) possess greater than a critical mass of SNM and engage in enriched uranium processing, fabrication of uranium fuel or fuel assemblies, uranium enrichment, enriched uranium hexafluoride conversion, plutonium processing, fabrication of mixed-oxide fuel or fuel assemblies, scrap recovery of SNM, or any other FCF activity that the Commission determines could significantly affect public health and safety; or (2) engage in uranium hexafluoride conversion or uranium hexafluoride deconversion.

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

Key Features of the Proposed Rule

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

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

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

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

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

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

The proposed rule's graded, consequence-based approach to the protection of digital assets limits the burden on FCF licensees by allowing them to focus their cyber security efforts on protecting against only those cyber threats that could compromise VDAs and result in a defined consequence of concern. This approach reduces the number of digital assets at FCFs that licensees are required to protect. The proposed rule also avoids a stand-alone focus on cyber security by allowing licensees to take credit for an alternate means of preventing a consequence of concern through the integration of cyber security requirements with the physical security measures currently employed at FCFs.

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

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

Implementation of the Proposed Rule

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

Coordination with the Advisory Committee on Reactor Safeguards

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

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

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

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

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

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

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

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

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

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

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

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

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

Stakeholder Interactions

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

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

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

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

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

Implementing Guidance

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

Potential Policy Considerations

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

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

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

Second, the safety consequences of concern defined in the proposed rule include events that may only impact on-site personnel. This is a departure from other security rulemakings in that there is not usually a requirement to specifically protect on-site personnel from the consequences of a security threat. During the development of the safety consequences of concern defined in the proposed rule, the NRC staff considered several options regarding potential consequence thresholds. Specifically, the staff considered thresholds to require protection against a cyber attack resulting in: (1) only off-site safety (i.e., radiological and chemical) consequences; (2) off-site safety consequences and on-site radiological consequences; or (3) off-site safety consequences, on-site radiological consequences, and on-site chemical consequences. While for other types of licensees (e.g., operating reactor licensees) the NRC has typically focused on establishing performance objectives/requirements that are protective of the public rather than on-site personnel, the staff determined that option (3) was more consistent with the existing regulatory approach used for FCF licensees. The inclusion of a threshold for on-site radiological consequences in the proposed rule addresses cyber attacks capable of causing a criticality, which would be a significant on-site event but may have no off-site impacts. By also including thresholds for on-site chemical consequences (e.g., an acute chemical exposure to a single worker that could lead to irreversible or other serious, long-lasting health effects) in the proposed rule, the identification of digital assets is tied to the existing performance requirements in 10 CFR 70.61. The benefits and costs of this approach are discussed in the draft regulatory and backfit analyses.

In contrast to the approach taken in the proposed rule, other regulatory frameworks, such as the Department of Homeland Security's Chemical Facility Anti-Terrorism Standards (CFATS), establish minimum quantities of chemicals as a threshold for applicability of facility-wide protection requirements. Under CFATS, a facility does not need to establish protections for chemicals of interest in amounts below these minimum quantity thresholds because malevolent acts could not create a toxicity, flammability, or explosion hazard that would "affect populations within and beyond a facility." In essence, the CFATS regulatory framework is consequence-based, however, it is different from the graded, consequence-based approach used in the proposed cyber security rule in that the rule defines the consequence threshold (e.g., a radiological exposure of 25 rem or greater for any individual, an intake of 30 mg or greater of uranium in soluble form for any individual outside the controlled area, or an acute chemical exposure that could lead to irreversible or other serious, long-lasting health effects for any individual), whereas the CFATS consequence thresholds are not defined.

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

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

COMMITMENT:

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

RESOURCES:

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

RECOMMENDATIONS:

That the Commission:

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

2. Note:

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

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

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

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

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

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

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

COORDINATION:

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

/RA/

Victor M. McCree
Executive Director
for Operations

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

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

DISTRIBUTION:
EDO Control RidsEdoMailCenter RidsNSIRMailCenter

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

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

OFFICIAL RECORD COPY

[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.

Draft Backfit Analysis and Documented Evaluation for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR 73.53)

U.S. Nuclear Regulatory Commission

Office of Nuclear Material Safety and Safeguards

2017

TABLE OF CONTENTS

LIST OF TABLES

ABBREVIATIONS AND ACRONYMS

ADAMS	Agencywide Documents Access and Management System
AEA	Atomic Energy Act of 1954, as amended
AIS	Abbreviated Injury Scale
CFR	Code of Federal Regulations
DBT	design basis threat
FAA	U.S. Federal Aviation Administration
FCF	fuel cycle facility
FR	*Federal Register*
FRN	*Federal Register* notice
HF	hydrogen fluoride
IROFS	items relied on for safety
ICM	interim compensatory measure (orders)
ISA	integrated safety analysis
MC&A	material control and accounting
NIST	National Institute for Standards and Technology
NRC	U.S. Nuclear Regulatory Commission
NSI	national security information
RD	restricted data
SNM	special nuclear material
SSNM	strategic special nuclear material
TCM	temporary compensatory measure
UF_6	uranium hexafluoride
VDA	vital digital asset

I. INTRODUCTION

I.1 Background

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

In addition, the proposed rule distinguishes FCF licensees according to the category of the facility: (1) 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material," licensees authorized to possess or use a formula quantity of strategic special nuclear material (SSNM) as defined in 10 CFR 73.2, "Definitions," (Category I FCF licensees); (2) 10 CFR Part 70 licensees authorized to possess or use SNM of moderate strategic significance as defined in 10 CFR 73.2 (Category II FCF licensees); (3) 10 CFR Part 70 licensees authorized to possess or use SNM of low strategic significance as defined in 10 CFR 73.2 (Category III FCF licensees); and (4) 10 CFR Part 40 licensees authorized to perform uranium hexafluoride conversion or deconversion (conversion and deconversion facility licensees). The NRC has developed a detailed consideration of benefits and costs in the draft regulatory analysis, "Draft Regulatory Analysis for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR 73.53)" (Draft RA) (Agencywide Documents Access and Management System (ADAMS) Accession No. ML16320A452), for these facilities to implement the proposed rule.

The Atomic Energy Act of 1954, as amended, (AEA) provides the NRC with the general authority to conduct this rulemaking. The authority citations in 10 CFR Part 40 and Part 70 refer to AEA Section 161, "General Provisions," which authorizes the NRC to establish rules, regulations, or orders governing the possession and use of special nuclear material, source material, and byproduct material. Additionally, the authority citations in 10 CFR Part 40 and Part 70 refer to AEA Section 63, "Domestic Distribution of Source Material," and Section 53, "Domestic Distribution of Special Nuclear Material," respectively. These two sections of the AEA require that the NRC establish, by rule,

minimum criteria for the issuance of specific or general licenses for the distribution of source material and special nuclear material, depending upon the degree of importance to the common defense and security or to the health and safety of the public with respect to: (1) the physical characteristics of the material to be distributed; (2) the quantities of material to be distributed; and (3) the intended use of the material to be distributed.

The proposed rule would require licensees to identify digital assets whose compromise by a cyber attack would result in specific consequences of concern to public health and safety and the common defense and security. The thresholds for each of these consequences of concern are informed by existing safety, security, and safeguards performance criteria in 10 CFR Parts 70, 73, 74, "Material Control and Accounting of Special Nuclear Material," and 95 "Facility Security Clearance And Safeguarding of National Security Information and Restricted Data." Furthermore, the proposed rule would require cyber security controls to be applied only to vital digital assets (VDA) (i.e., those for which no alternate means exists to prevent the consequence of concern if compromised). Consideration of alternate means allows FCF licensees to credit other site-specific security and safety measures that either protect digital assets or prevent the consequence of concern in lieu of employing measures to protect against the consequence of concern by implementing cyber security controls.

The FCF facilities whose operations will be impacted by this proposed rulemaking are listed in the table below and are grouped by their license category.

Table I-1 Facilities subject to the proposed requirements in 10 CFR 73.53

Category of FCF Licensee	Name of Facility	Facility Activity
Category I	Babcock & Wilcox Nuclear Operations Group	Fuel Fabrication
	Nuclear Fuel Services	Fuel Fabrication
	Shaw AREVA MOX Services, LLC	Fuel Fabrication – Mixed Oxide
Category II	None	N/A
Category III, with Classified Information	Louisiana Energy Services, URENCO USA	Uranium Enrichment – Gas Centrifuge
Category III, without Classified Information	AREVA, Richland, Inc.	Fuel Fabrication
	Global Nuclear Fuel – Americas, LLC	Fuel Fabrication
	Westinghouse Electric Company, LLC	Fuel Fabrication
Conversion and Deconversion	Honeywell International, Inc.	Uranium Hexafluoride Conversion

As noted in the Draft RA, Appendix A, "Estimated Operational Years Remaining for Fuel Cycle Facility Licensees," four proposed facilities that would be subject to the proposed rule (i.e., American Centrifuge Plant, GE-Hitachi, Eagle Rock Enrichment Facility, and International Isotopes Fluorine Products, Inc.) have received NRC licenses but have no projected construction or operation schedule. These licenses expire between 2037 and 2052. Costs for these FCF licensees are uncertain, and therefore not included in this backfit analysis, because the NRC is not able to determine if, or when, these entities

would possess licensed material and, therefore, be subject to the provisions of the proposed rule. However, if these licensees proceeded to construct and operate FCFs consistent with their licenses, the costs would be consistent with their category of facility, as discussed in Sections III–V of this backfit analysis. Future discounting would depend upon when such a facility was required to comply with the proposed rule. In addition, the Commission issued a construction authorization to the license applicant for the Mixed Oxide Fuel Fabrication Facility (MOX facility) on March 30, 2005. A license application to possess and use byproduct and SNM is currently pending before the Commission. Current and future license applicants generally do not have backfitting protection. But for the purpose of this backfit analysis, the staff has also included the MOX facility in its evaluation.

The listing of FCF licensees compiled in Table I-1, "Facilities subject to the proposed requirements in 10 CFR 73.53," are the same as those listed in the Draft RA, Table 3-1, "Impacted Entities." In addition, applicable considerations in the Draft RA, Appendix A, "Estimated Operational Years Remaining for Fuel Cycle Facility Licensees," were used in this draft backfit analysis. The FCFs licensed under 10 CFR Part 70 are grouped by category based on the quantity and type of special nuclear material they are licensed to possess (i.e., as defined in 10 CFR 70.4, "Definitions," and 73.2). The uranium hexafluoride conversion facility licensed under 10 CFR Part 40 is listed in a separate category.

I.2 Backfit requirements

In accordance with the requirements in 10 CFR 70.76, "Backfitting," this document presents the NRC staff's evaluation of the new provisions of the proposed cyber security rule. The backfit analysis examines the impacts of the proposed rule relative to current requirements, including existing regulations and orders. It provides the staff's analysis of which provisions of the proposed rule constitute backfits on protected entities, whether any of these proposed backfits are subject to an exception to the backfit rule's analysis requirement in 10 CFR 70.76(a)(3), and whether those proposed backfits not subject to an exception to the backfit analysis requirement provide a cost-justified substantial increase in overall protection of public health and safety or common defense and security.

As stated in 10 CFR 70.76(a)(1), backfitting is defined as, "the modification of, or addition to, systems, structures, or components of a facility; or to the procedures or organization required to operate a facility; any of which may result from a new or amended provision in the Commission rules or the imposition of a regulatory staff position interpreting the Commission rules that is either new or different from a previous NRC staff position." The proposed provisions of 10 CFR 73.53, "Requirements for cyber security at nuclear fuel cycle facilities," are a backfit.

The NRC may impose a backfit only if it performs a backfit analysis in accordance with 10 CFR 70.76(a)(2), unless one of four specified exceptions apply. The backfit analysis must demonstrate, in accordance with 10 CFR 70.76(a)(3), "that there is a substantial increase in the overall protection of the public health and safety or the common defense and security to be derived from the backfit and that the direct and indirect costs of implementation for the facility are justified in view of this increased protection."

The four exceptions to the requirements to prepare a backfit analysis are set forth in 10 CFR 70.76(a)(4). The first two exceptions, provided in 10 CFR 70.76(a)(4)(i)-(ii), are related to compliance, and apply if a "modification is necessary to bring a facility into compliance with Subpart H of [Part 70]," or, "...a modification is necessary to bring a facility into compliance with a license or the rules or orders of the Commission, or into conformance with written commitments by the licensee." These first two exceptions do not apply to the proposed provisions. The third and fourth exceptions in 10 CFR 70.76(a)(4)(iii)-(iv) are related to actions necessary to ensure adequate protection or to actions that involve defining or redefining adequate protection. The requirements in 10 CFR 70.76(a)(4)(iii) apply to some of the provisions proposed in this rule. Its application is discussed in detail below.

I.3 Existing requirements

The NRC currently lacks a comprehensive regulatory framework for addressing cyber security at FCFs. Subsequent to the events of September 11, 2001, the NRC issued Interim Compensatory Measure (ICM) Orders that required FCF licensees to evaluate computer and communications networks and address safety and security vulnerabilities as necessary. However, the NRC did not provide guidance on how to implement the cyber security requirement in the ICM Orders. Additionally, in Section 651 of the Energy Policy Act of 2005, Congress directed the Commission to initiate a rulemaking to revise the design basis threats (DBTs) set forth in 10 CFR 73.1, "Purpose and scope." 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, "General performance objective and requirements," Category I FCF licensees must maintain a physical protection system designed to protect against both the DBT for radiological sabotage and the DBT for theft or diversion of formula quantities of SSNM. Both DBTs include a cyber attack as a method that may be exploited by adversaries. However, current NRC physical protection requirements do not set forth specific provisions for addressing cyber attacks at Category I FCFs. Furthermore, no NRC guidance specifically discusses requirements or strategies for protecting against cyber attacks for FCFs.

The NRC staff directed FCF licensees to consider cyber security protections through the ICM Orders, which were issued in 2002 and 2003. The primary concern of the ICM Orders was a physical attack; however, the ICM Orders contained a generic requirement for licensees to consider cyber security and address safety and security vulnerabilities "as necessary." Licensees were required to evaluate computer and communication networks for concerns related to "cyber terrorism." 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. The cyber security requirements in the DBTs and ICM Orders for FCF licensees were imposed as an early recognition of the growing cyber threat environment. However, corresponding changes were not required to be made to facilities' licensing bases (e.g., security plan, license conditions, and integrated safety analysis). In

addition, no NRC enforcement actions have been taken on cyber security-related issues for FCF licensees.

In addition to meeting the requirements in the DBTs and ICM Orders, FCF licensees that hold classified information (i.e., Category I and Category III FCF enrichment licensees) are required to meet the security requirements in 10 CFR Part 95 and must maintain a facility security clearance because they process and store National Security Information (NSI) and/or Restricted Data (RD). The security requirements in 10 CFR Part 95 provide for the protection of classified information "while unattended" (10 CFR 95.25, "Protection of National Security Information and Restricted Data in storage") and "while in use" (10 CFR 95.27, "Protection while in use"). An additional provision in 10 CFR 95.35, "Access to matter classified as National Security information and Restricted Data," provides requirements for controlling access to classified information to only authorized individuals. These requirements provide for the protection of classified information which includes protection against the loss or unauthorized disclosure (i.e., compromise), including from a cyber attack. However, Part 95 and related guidance do not provide specific cyber security provisions for the protection of digital assets for the required protection of classified information (e.g., electronic door locks, surveillance cameras, and intrusion detection systems). If not adequately protected, these physical security digital assets have the potential to be compromised by a cyber attack and may not be reliable or available to perform their intended security function during an event (i.e., may result in a security consequence of concern).

The DBTs, ICM Orders, 10 CFR Part 95, and their associated guidance documents do not provide FCF licensees with specific provisions for protection against cyber attacks or for the establishment of a formal cyber security program beyond the general requirements discussed above. Furthermore, no additional requirements or guidance have been developed by the NRC to describe how FCF licensees should respond to the evolving cyber security threat environment. Additional information on the potential vulnerabilities of FCF licensees in the current cyber security threat environment is provided in the Draft RA, Appendix B "Vulnerability of Fuel Cycle Facilities to a Cyber Threat." Potential cyber security vulnerabilities observed at FCFs by the NRC staff during site visits increase the likelihood that a cyber attack could cause a consequence of concern, given the recent global rise in: (1) the number of cyber attacks; (2) the level of sophistication of such attacks; (3) the potential for these attacks to impact digital assets, including digital assets used at FCFs; and (4) the demonstration of these attacks to produce kinetic effects.

The requirements for FCF licensees contained in 10 CFR Parts 20, "Standards for Protection Against Radiation," 40, and 70 provide for safe operations. In addition, the integrated safety analysis (ISA) requirements in 10 CFR Part 70 provide for engineered or administrative controls, designated as items relied on for safety (IROFS), to ensure that each IROFS is available and reliable to perform its intended function when needed and meets the performance requirements of 10 CFR 70.61, "Performance requirements." However, these safety requirements do not include specific consideration of malicious actors. The potential for a cyber attack to impact safety and security systems at a FCF differs from those associated with a physical attack. As discussed in the Draft RA, Appendix B, a cyber attack can be carried out remotely, by multiple parties, over an extended period of time. During site visits at various FCFs, the NRC staff observed digital IROFS being used to perform certain safety functions that were susceptible to potential attack vectors. If not adequately protected, these IROFS

have the potential to be compromised by a cyber attack and may not be available or reliable to perform their intended safety function during an event (i.e., may result in a safety consequence of concern).

I.4 Proposed requirements for cyber security at fuel cycle facilities

The proposed 10 CFR 73.53(b), "Cyber security program performance objectives," 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 one or more of the consequences of concern identified in 10 CFR 75.53(c), "Consequences of concern."

I.4.1 Consequences of Concern

The licensee's cyber security program would be required to provide for protection against the following four types of consequences of concern:

- Latent consequences of concern – DBT, as identified in 10 CFR 73.53(c)(1) (hereafter referred to as latent DBT), would only apply to Category I FCF licensees and is discussed in Section III of this backfit analysis.

- Latent consequences of concern – safeguards, as identified in 10 CFR 73.53(c)(2) (hereafter referred to as latent safeguards), would only apply to Category II FCF licensees, for which none currently exist. Therefore, this consequence of concern is not discussed in this backfit analysis.

- Active consequences of concern – safety, as identified in 10 CFR 73.53(c)(3) (hereafter referred to as active safety), would apply to radiological and chemical consequences for FCF licensees and is discussed in Section IV of in this analysis.

- Latent consequences of concern – safety and security, as identified in:

  - 10 CFR 73.53(c)(4)(i)-(iii) (hereafter referred to as latent safety), would consider radiological and chemical consequences applicable to all FCF licensees, and is discussed in Section IV of this backfit analysis; and

  - 10 CFR 73.53(c)(4)(iv) (hereafter referred to as latent security), would consider the loss or unauthorized disclosure of classified information and matter for certain FCF licensees, and is discussed in Section III of this backfit analysis.

The distinction between active and latent consequences of concern is that, 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 proposed regulatory thresholds. 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 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 the common defense and security.

I.4.2 Cyber Security Program

In order to meet the cyber security program performance objectives in the proposed 10 CFR 73.53(b), the cyber security program would be required to include the features described below in items a – k.

a. The proposed 10 CFR 73.53(d)(1) would require FCF licensees to establish and maintain a Cyber Security Team to ensure the implementation and maintenance of the cyber security program. The Cyber Security Team would need to be adequately structured, staffed, trained, qualified, and equipped to implement the cyber security program. This provision would ensure that the licensee establishes a team with sufficient knowledge and authority to implement and maintain a cyber security program to protect against the consequences of concern.

b. The proposed 10 CFR 73.53(d)(2) would require FCF licensees to 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. The cyber security controls would prevent the types of consequences of concern specific to the facility, as specified in 10 CFR 73.53(c).

c. The proposed 10 CFR 73.53(d)(3) would require FCF licensees, specific to the category of the facility, to identify digital assets that if compromised by a cyber attack, would result in a latent DBT, latent safeguards, active safety, latent safety, or latent security consequence of concern.

d. The proposed 10 CFR 73.53(d)(4) would require FCF licensees to identify VDAs. A digital asset is vital if no alternate means that is protected from a cyber attack can be credited to prevent a consequence of concern, as specified in 10 CFR 73.53(c).

   A FCF licensee may credit alternate means to prevent a consequence of concern associated with a digital asset identified through the proposed 10 CFR 73.53(d)(3). This provision to credit alternate means or identify a VDA would enable a FCF licensee to clarify the scope of its cyber security program and provide the NRC with assurance that digital assets, whose compromise by a cyber attack would result in a consequence of concern, have been considered.

e. The proposed 10 CFR 73.53(d)(5) would require FCF licensees to establish and maintain implementing procedures that document the measures taken to address the performance specifications associated with the applicable cyber security controls.

   – The proposed 10 CFR 73.53(d)(5)(i) would require FCF licensees to identify the specific cyber security controls that would be applied to each VDA.

   – The proposed 10 CFR 73.53(d)(5)(ii) would require FCF with VDAs to establish and maintain implementing procedures that document the measures taken to address the performance specifications of the cyber security controls.

f. The proposed 10 CFR 73.53(d)(6) would require FCF licensees with VDAs to provide and document temporary compensatory measures (TCMs) in the event measures taken to address cyber security controls become degraded. A TCM would provide a temporary solution for securing a VDA until permanent controls are properly implemented and verified. The TCMs would ensure that the cyber security program performance objectives continue to be met when cyber security controls cannot be applied or fail to perform as intended. The provisions of 10 CFR 73.53(d)(6) would also require a licensee to document and track TCMs until no longer needed.

g. The proposed 10 CFR 73.53(e), "Cyber security plan," would require FCF licensees to establish, implement, and maintain a site-specific cyber security plan that describes how the cyber security program performance objectives are met, and to provide for incident response for a cyber attack capable of causing a consequence of concern.

   The cyber security plan would describe how the licensee satisfies the requirements of the proposed 10 CFR 73.53 (herein described by items a – k of this section), manages the cyber security program, and provides incident response for a cyber attack capable of causing a consequence of concern. The plan would provide: methodology for the identification and protection of VDAs; the management measures for the cyber security program; and a description of the approach for responding to a cyber attack capable of causing a consequence of concern.

h. The proposed 10 CFR 73.53(f), "Configuration management," would require FCF licensees to establish and maintain a configuration management system to ensure the cyber security program objectives remain satisfied. A FCF licensee would evaluate any previously unidentified digital assets, or modifications to existing digitals assets that are included in the cyber security program, prior to being implemented. A facility's VDAs may change over time. There is a continued potential for the exploitation of new vulnerabilities caused by configuration changes that could result in a consequence of concern. The configuration management system would ensure that changes to the facility are evaluated prior to implementation and do not adversely impact the ability to meet the cyber security program requirements.

i. The proposed 10 CFR 73.53(g), "Review of the cyber security program," would require FCF licensees to periodically review the effectiveness of the cyber security program. Category I FCF licensees would perform a review of the cyber security program as a component of the annual security program review in accordance with the requirements of 10 CFR 73.46(g)(6). All other FCF licensees would perform a review of the cyber security program at least every 36 months.

   This review would include an audit of the effectiveness of the cyber security program including, but not limited to, applicable cyber security implementing procedures, controls, VDA determinations, and defensive architecture. The findings, deficiencies, and recommendations from this review would be tracked, addressed in a timely manner, and documented in a report to the licensee's facility manager and corporate management. This provision would ensure that FCF licensees periodically confirm that the cyber security program meets the required performance objectives (i.e., detect, protect against, and respond to a cyber attack capable of causing a consequence of concern).

j. The proposed 10 CFR 73.53(h), "Event reporting and tracking," would require FCF licensees to notify the NRC Operations Center of certain cyber security events and internally track other cyber events. Licensees 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, within 24 hours of discovery, to record and track to resolution the failure, compromise, vulnerability, or degradation that resulted in a decrease in effectiveness of a cyber security control. Furthermore, Category I and II FCF licensees would be required to record, within 24 hours of discovery, if a cyber attack compromises a VDA associated with a consequence of concern related to nuclear material control and accounting (i.e., 10 CFR 73.53(c)(1)(iii) or (c)(2)(ii)).

k. The proposed 10 CFR 73.53(i), "Records," would require FCF licensees to maintain certain documentation as records. This provision would require FCF licensees to retain supporting technical documentation demonstrating compliance with the requirements of 10 CFR 73.53. This provision would also require FCF licensees to maintain and make available for inspection all records, reports, and documents required to be kept by the Commission until termination of the license or for at least 3 years after the records are superseded.

These proposed requirements would establish a cyber security program capable of protecting against a consequence of concern from the compromise, due to a cyber attack, of digital assets. This is accomplished through programmatic requirements for FCF licensees to establish a basic cyber security infrastructure (e.g., plan, team, and controls) and provisions (e.g., analysis, controls, implementing procedures, and TCMs) to identify and protect VDAs specific to the category of facility. The proposed rule requires FCF licensees to detect, protect against, and respond to a cyber attack capable of causing specific consequences of concern.

I.5 Entities subject to backfit protection

The proposed rule would impact FCF licensees subject to: (1) 10 CFR 70.60; or (2) the requirements of 10 CFR Part 40 for operation of a uranium hexafluoride conversion or deconversion facility. With respect to 10 CFR 70.60, only those licensees subject to the requirements in 10 CFR Part 70, Subpart H, "Additional Requirements for Certain Licensees Authorized To Possess a Critical Mass of Special Nuclear Material," are afforded backfit protection.

I.5.1 Conversion and Deconversion facility licensees

FCFs licensed under 10 CFR Part 40 (i.e., uranium hexafluoride conversion and deconversion facilities) are not subject to backfitting protection. Thus, backfitting considerations need not be addressed by the NRC in developing the proposed rule for these facilities. However, the NRC has included a consideration benefits and costs for these facilities in the Draft RA and finds that imposition of the proposed requirements on such facilities is cost-beneficial.

I.5.2 Part 70 FCF licensees

As previously noted, FCFs licensed under 10 CFR Part 70 and subject to the requirements of Subpart H are subject to the backfitting protections in 10 CFR 70.76. These FCF licensees include three facility types: (1) those authorized to possess or use a formula quantity of SSNM (Category I FCF licensees); (2) those authorized to possess or use SNM of moderate strategic significance (Category II FCF licensees); and (3) those authorized to possess or use special nuclear material of low strategic significance (Category III FCF licensees). Currently, the NRC has no licensed Category II FCF licensees. Therefore, this type of facility is not considered in this backfit analysis.

I.6 Considerations of backfit for existing facilities

This backfit evaluation is based in part on the adequate protection exception to the backfit analysis requirement in 10 CFR 70.76(a)(4)(iii), 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 required to protect against: (1) the DBTs in accordance with 10 CFR 73.20, or (2) the loss or unauthorized disclosure of classified information or matter (classified information) in accordance with 10 CFR Part 95. Both of these are identified in the proposed rule as consequences of concern. The cost-justified portion of the proposed rule applies to the active and latent safety consequences of concern (i.e., radiological exposure, uranium intake, and acute chemical exposure). The portions of the rule that apply to the latent safeguards consequence of concern do not require a backfit justification because they apply to Category II FCF licensees, of which none are currently licensed. The portions of the rule that apply to FCFs licensed under 10 CFR Part 40 do not require a backfit justification because the corresponding portions of the regulations do not afford these facilities backfit protection.

This backfit analysis considers each FCF licensee impacted by the proposed rule. For the purpose of this backfit analysis, FCF licensees are subdivided into the five facility categories below, based on the applicable types of potential consequences of concern described in the proposed paragraph 73.53(c).

1) Category I FCF licensees:
    - latent DBT;
    - active safety;
    - latent safety; and
    - latent security.
2) Category II FCF licensees (of which there are currently none):
    - latent safeguards;
    - active safety;
    - latent safety; and
    - latent security.

3) Category III FCF licensees with classified information:
    - o active safety;
    - o latent safety; and
    - o latent security.
4) Category III FCF licensees without classified information:
    - o active safety; and
    - o latent safety.
5) Conversion and deconversion facility licensees (which are not afforded backfit protection):
    - o active safety; and
    - o latent safety.

All FCF licensees in these five facility categories would be required to implement a cyber security program to meet the program performance objectives of the proposed rule. As listed above, FCF licensees are subdivided into categories in order to delineate the backfit exceptions and analyses associated with each consequence of concern. For example, Category I FCF licensees would have cyber security program requirements based on the latent DBT and latent security consequences of concern. Both of these security aspects of the program are subject to the backfit analysis exception for requirements necessary for adequate protection. Category I FCF licensees would also have cyber security program requirements based on active safety and latent safety consequences of concern. These safety aspects of the program are not subject to such an exception and, as demonstrated in this backfit analysis, the associated requirements provide a substantial increase in safety and are cost-justified. Therefore, grouping the FCF licensees by these categories facilitates the NRC's backfit evaluation of the proposed rule.

As part of the backfit analysis, the NRC staff considered which requirements of the proposed rule are subject to the adequate protection exception and which are not. For each category of facility, Table I-2 identifies the estimated costs associated with protection against each type of consequence of concern. The estimates in the table are further categorized by whether protecting against a particular consequence of concern is necessary for adequate protection and is in accord with the common defense and security, or if a backfit analysis (10 CFR Part 70.76(a)(3)) is required.

Table I-2 Percentage of costs estimated to implement proposed requirements necessary for adequate protection versus those subject to a backfit analysis

Category (Cat.) of FCF Licensee	Allocations of costs to implement a cyber security program to detect, protect against, and respond to a cyber-attack capable of causing the specified type of consequence of concern					Total percent of Effort by Type of Backfit Justification
	Type of Backfit Justification	DBT* 10 CFR 73.53 (c)(1)	Safeguards** 10 CFR 73.53(c)(2)	Latent Security* 10 CFR 73.53 (c)(4)(iv)	Active Safety or Latent Safety*** 10 CFR 73.53(c)(3) and 73.53 (c)(4)(i)-(iii)	
Cat. I	Adequate Protection	50%	0%	25%	0%	75%
	Cost Justified	0%	0%	0%	25%	25%
Cat. II**	Adequate Protection	0%	0%	0%	0%	0%
	Cost Justified	0%	0%	0%	0%	0%
Cat. III with Classified Information	Adequate Protection	0%	0%	75%	0%	75%
	Cost Justified	0%	0%	0%	25%	25%
Cat. III without Classified Information***	Adequate Protection	0%	0%	0%	0%	0%
	Cost Justified	0%	0%	0%	100%	100%
Conversion and Deconversion**	Adequate Protection	0%	0%	0%	0%	0%
	Cost Justified	0%	0%	0%	100%	100%

* Further discussed under Exceptions to the Backfit (adequate protection)
** Further discussed under Proposed Requirements that Do Not Constitute Backfitting
*** Further discussion under Cost Justified Substantial Increase in Overall Protection

The following considerations informed the development of the percentages in Table I-2

- For Category I FCF licensees, 75 percent of the total costs estimated to satisfy the proposed rule would be based on requirements associated with latent DBT and latent security consequences of concern (i.e., justification based on adequate protection against the DBTs and security consequences of concern). The other apportioned 25 percent of the estimated costs would be required to satisfy proposed requirements associated with active safety or latent safety consequences of concern (i.e., backfit analysis is required).

- For Category III FCF licensees with classified information, 75 percent of the total costs estimated to satisfy the proposed rule would be based on requirements associated with latent security consequence of concern (i.e., justification based on adequate protection against the loss or unauthorized disclosure of classified information). The other apportioned 25 percent of the estimated costs would be necessary to satisfy the proposed requirements associated with active safety or latent safety consequences of concern (i.e., backfit analysis is required). This ratio is based on NRC observations that the majority of the digital assets associated with safety functions at these facilities reside on classified networks authorized by the U.S. Department of Energy, which are excepted from the proposed rule. Unlike those digital assets associated with safety functions on the classified networks, most physical security systems are not on classified networks. Therefore, the staff finds that a higher proportion of potential VDAs at these facilities are associated with the security consequences of concern.

- All of the costs for Category III FCF licensees without classified information are required to satisfy the proposed rule requirements associated with active safety or latent safety consequences of concern (i.e., backfit analysis is required).

- As discussed previously in this Section, FCFs licensed under 10 CFR Part 40 are not subject to backfit protection. As noted in the Draft RA, the costs associated with implementing the proposed rule for these facilities is entirely due to the active and latent safety consequences of concern.

This backfit analysis has been conducted for each of the following provisions of the proposed rule, grouped by subject matter:

- performance objectives – 10 CFR 73.53(b);
- Cyber Security Team – 10 CFR 73.53(d)(1);
- cyber security controls – 10 CFR 73.53(d)(2), (5)(i), and (6);
- identification of VDAs – 10 CFR 73.53(d)(3)-(4);
- protection of VDAs – 10 CFR 73.53(d)(5)(ii);
- cyber security plan – 10 CFR 73.53(e);
- configuration management – 10 CFR 73.53(f); and
- periodic program reviews – 10 CFR 73.53(g).

The proposed rule provisions that either amend existing information collection requirements or impose new information collection and reporting requirements (i.e., 10 CFR 73.53(a), "Introduction," (h), and (i)) are not included in the above list because information collection requirements are not subject to backfit analyses.

Table I-3 identifies an estimated percentage of the effort that would be needed to satisfy each provision of the proposed rule listed above. Since each provision of the proposed rule may address requirements associated with multiple consequences of concern, each provision may be required for either adequate protection, may be cost-justified, or both. In certain cases (i.e., for certain classes of facilities), provisions of the proposed rule are justified by adequate protection. In those cases, Table I-3 assigns 100 percent of the cost to adequate protection, even though those provisions may also be required under the cost-justified provisions of the proposed rule (i.e., provisions justified by adequate protection are not included in the cost-justified considerations).

In certain cases, the costs associated with a provision of the proposed rule are applicable to multiple consequences of concern. These costs are allocated, as appropriate, to those provisions required for adequate protection or to those provisions subject to a backfit analysis. For example, for Category I FCF licensees, the costs associated with the requirement to identify VDAs is partially allocated for adequate protection and partially allocated as cost-justified, since VDAs could be associated with the latent DBT, latent security, active safety, or latent safety consequences of concern. Therefore, with respect to the protection of VDAs for Category I FCF licensees, the cost breakdown in Table I-3 is listed as 75 percent necessary for adequate protection (i.e., latent DBT or latent security consequences of concern) and 25 percent necessary for a cost-justified substantial increase in overall protection (i.e., active safety or latent safety consequences of concern).

Cost Allocation

The NRC staff's assessment of cost allocation is based on site visits and overall assessments of each facility class, as well as input from stakeholders. For Category I FCF licensees, the estimate of 75 percent of total costs to implement the proposed rule is attributed to adequate protection. This estimate is based upon the provisions for protection against consequences of concern associated with the DBTs (50 percent) and associated with the security of classified information (25 percent). Those requirements needed for an increase in overall safety are estimated to comprise the remaining 25 percent of total costs and are included in the backfit analysis. Specifically, the programmatic provisions of the proposed rule (i.e., meeting the performance objectives, creating an appropriate cyber security team, creating a cyber security plan, and implementing configuration management) are required for those consequences of concern associated with ensuring adequate protection for Category I FCF licensees.

For Category III FCF licensees with classified information, the estimate of 75 percent of total costs to implement the proposed rule is attributed to adequate protection. This estimate is based upon the provisions for protection against consequences of concern associated with the security of classified information. This estimate is informed by NRC observations that the majority of the digital assets associated with safety functions at these facilities reside on classified networks authorized by the U.S. Department of Energy, and are excepted from the proposed rule. Unlike those digital assets associated with safety functions on the classified networks, most physical security systems are not on classified networks. Therefore, the NRC staff concluded that a higher proportion of potential VDAs at Category III FCFs with classified information are associated with the security consequences of concern. Those requirements needed for an increase in overall safety are estimated to comprise the remaining 25 percent of total costs and are included in the backfit analysis. Specifically, the programmatic provisions of the proposed rule (i.e., meeting the performance objectives, creating an appropriate cyber security team, creating a cyber security plan, and implementing configuration management) are required for those consequences of concern necessary for adequate protection for Category III FCF licensees with classified information.

In addition, Category II FCF licensees and conversion and deconversion facility licensees are listed in the tables for completeness. There are no backfitting considerations associated with these types of facilities. Currently, there are no

Category II FCF licensees. In addition, conversion and deconversion facility licensees authorized under 10 CFR Part 40 are not afforded backfit protection.

Table I-3 Breakdown of how costs are considered in the backfit analysis

Category (Cat.) of FCF Licensee	Type of Backfit Justification	Percentage of the Backfit Justification Required Based on the Major Cyber Security Program Elements							
		Performance objectives 10 CFR 73.53(b)	Cyber Security Team 10 CFR 73.53(d)(1)	Cyber security controls 10 CFR 73.53(d)(2), (5)(i), and (6)*	Identification of VDAs 10 CFR 73.53(d)(3)-(4)*	Protection of VDAs 10 CFR 73.53(d)(5)(ii)*	Cyber security plan 10 CFR 73.53(e)	Configuration management 10 CFR 73.53(f)*	Periodic program reviews 10 CFR 73.53(g)*
Cat. I	Adequate Protection	100%	100%	75%	75%	75%	100%	75%	75%
	Cost Justified	0%	0%	25%	25%	25%	0%	25%	25%
Cat. II	None								
Cat. III with Classified Information	Adequate Protection	100%	100%	75%	75%	75%	100%	75%	75%
	Cost Justified	0%	0%	25%	25%	25%	0%	25%	25%
Cat. III without Classified Information	Adequate Protection	0%	0%	0%	0%	0%	0%	0%	0%
	Cost Justified	100%	100%	100%	100%	100%	100%	100%	100%
Conversion and Deconversion	None								

* The values for these proposed rule components are drawn from the analysis in Table I-2

II. PROPOSED REQUIREMENTS THAT DO NOT CONSTITUTE BACKFITTING

This backfit analysis examines the proposed cyber security requirements for applicable FCF licensees. Those proposed provisions that potentially constitute backfitting are described later in this document. Proposed requirements that do not constitute potential backfits include those that fall into one or more of the following categories, as discussed in NUREG-1409, "Backfitting Guidelines" (ADAMS Accession No. ML032230247), and described in the definition of backfitting in 10 CFR 70.76(a)(1):

- Administrative matters
  Revisions that make minor administrative changes, such as correction of typographic errors, correction of inconsistencies, relocating requirements from one section to another, and combining existing requirements into a single section.

- Information collection and reporting requirements
  Revisions that either amend existing information collection and reporting requirements or impose new information collection and reporting requirements, which are not themselves considered to be backfits.

- Clarifications
  Revisions that clarify current requirements to assure consistent understanding and implementation of the NRC's original intent for these requirements. These revisions remove ambiguities that produce regulatory uncertainty without changing the underlying requirements stated in the associated sections.

- Permissive relaxations or voluntary alternatives
  Revisions that permit, but do not require, relaxations or alternatives to current requirements (i.e., licensees are free to either comply with current requirements or adopt the relaxed requirements or a voluntary alternative as a binding requirement).

In properly codifying the proposed rule, administrative and conforming changes to other provisions of the regulations (e.g., 10 CFR Parts 40, 70, and 73) are also necessary. These proposed conforming changes to Parts 40, 70, and 73 are administrative in nature and therefore, do not constitute a backfit. The proposed provisions in 10 CFR 40.31(n), 40.35(g), 70.22(o), and 70.32(f) would require FCF licensees to submit their security plans and security plan changes to the NRC. The proposed conforming change to existing 10 CFR 73.46(g)(6) references the cyber security audits for existing Category I FCF licensees. These administrative, conforming changes would ensure FCF licensees comply with the proposed 10 CFR 73.53 and are not subject to backfit protection.

The proposed provision in 10 CFR 73.53(h) would require FCF licensees to report certain cyber security events to the NRC. The proposed provision in 10 CFR 73.53(i), would require FCF licensees to compile and maintain certain information for recordkeeping. These requirements of the proposed rule are administrative in nature, for information collection, or establish reporting requirements and therefore, are not separately subject to backfit protection.

III. EXCEPTIONS TO BACKFIT ANALYSIS

The NRC staff has identified specific provisions of the proposed rule, for certain FCF licensees, that it believes are necessary to ensure adequate protection, consistent with 10 CFR 70.76(a)(4), to the health and safety of the public and are in accord with the common defense and security. These provisions include cyber security requirements for the DBTs and related material control and accounting (MC&A) provisions that apply to Category I FCF licensees and to protecting classified information, applicable to Category I FCF licensees and Category III FCF licensees with classified information (e.g., enrichment facilities). The proposed rule largely clarifies existing cyber security requirements pertaining to the DBTs located in 10 CFR 73.1(a)(1) and 10 CFR 73.1(a)(2); MC&A in 10 CFR 74.51(a), "General performance objectives," for Category I FCF licensees; and the protection of classified information as required by Executive Order 13526, the Energy Reorganization Act of 1974, and as implemented in 10 CFR Part 95. These existing regulations contain requirements for adequate protection and common defense and security, including requirements for cyber security protection. However, as discussed in previous sections of this backfit analysis, these regulations do not specifically identify cyber security implementation criteria. Therefore, the proposed rule provides clarification for the cyber security program elements necessary to comply with the existing regulations and to achieve adequate protection. While the proposed 10 CFR 73.53 contains new requirements for licensees, as discussed below, those requirements involving the DBTs, MC&A, and Part 95 are necessary for adequate protection to clarify, formalize, and implement necessary protection against consequences of concern due to a cyber attack. As further discussed below, these requirements in the proposed rule are rooted in, and a necessary extension of, current requirements.

III.1 Why are certain cyber security requirements needed now for adequate protection?

The proposed rule would establish a cyber security program to provide for effective protection against cyber attacks. To meet the proposed performance requirements, the subject rule would require FCF licensees to implement programmatic requirements for: creating the appropriate Cyber Security Team, creating a cyber security plan, and implementing an appropriate configuration management system in order to prevent the consequences of concern. Although the consequences of concern differ based on facility type, the same program elements would be applied to accomplish the performance objectives. Application of the structured program would enable licensees to accomplish the performance objectives of preventing the consequences of concern to each type of facility. In its analysis of those elements of the proposed rule necessary for adequate protection, the NRC staff focused on the prevention of particular consequences of concern. Programmatic elements necessary for adequate protection would be used in the program to protect against all consequences of concern, including those analyzed in this backfit analysis. This is why costs associated with provisions of the proposed rule necessary for adequate protection, to the extent that they also provide program elements for protection against safety consequences of concern, are not considered in this backfit analysis beyond those marginal costs specific to the safety consequences of concern.

The proposed rule's provisions that would establish a cyber security program are necessary due to the evolving threat environment. As outlined in the Draft RA,

Appendix B, several events have occurred since 2010 that demonstrate the capability for an adversary to initiate a cyber attack that can cause physical damage to a FCF. Since 2015, two attacks have been initiated remotely against control and backup systems like those used by FCF licensees. These attacks resulted in alteration of site operations. One of these attacks led to a complete shutdown of the facility. Third-party analyses of these attacks have identified several vulnerabilities and lessons learned. These analyses informed the development of the proposed rule.

The proposed rule is needed now to define the elements of a cyber security program necessary to protect against consequences of concern. Observations made during NRC staff site visits indicate that FCF licensees recognize the potential threat of a cyber attack and have implemented a range of voluntary cyber security measures to address this threat. Implementing the proposed rule would assure that the resources licensees expend on cyber security measures will establish and continue to provide for adequate protection because they ensure the common defense and security.

This proposed rule would also facilitate clear and concise guidance on acceptable approaches for effective cyber security programs. The guidance associated with the proposed rule (Draft Regulatory Guide (DG) – 5062, "Cyber Security Programs for Nuclear Fuel Cycle Facilities," (ADAMS Accession No. ML16319A320)) describes acceptable approaches for establishing an effective cyber security program that would comply with the proposed rule. For example, it describes ways to implement the required elements of a cyber security program (e.g., Cyber Security Team, analysis to identify digital assets susceptible to a cyber security attack, controls to protect against a consequence of concern, implementing procedures, configuration management, and audit programs). Further, following the NRC's rulemaking process for the proposed provisions and associated guidance would ensure that stakeholders have substantial opportunity to inform their development.

As discussed above, specific cyber security requirements in existing regulations are generally absent for FCF licensees. The proposed rule would ensure that FCF licensees protect against the DBTs and prevent the loss or unauthorized disclosure of classified information in accordance with the common defense and security, generally as a continuation of existing requirements, while giving licensees flexibility to design and implement the program that is effective for their facility.

III.2 Proposed DBT requirements necessary for adequate protection

Category I FCF licensees are required to establish and maintain a physical protection system capable of protecting against the DBTs set forth in 10 CFR 73.1. In addition, the DBTs require licensees to defend against cyber attacks. However, as discussed in Section I.3 of this backfit analysis, current NRC regulations do not contain specific cyber security requirements to protect VDAs that perform the functions needed to prevent the following security and safeguards events:

- Radiological sabotage, as specified in 10 CFR 73.1(a)(1), at Category I FCF licensees;

- Theft and diversion of formula quantities of SSNM, as specified in 10 CFR 73.1(a)(2), at Category I FCF licensees; and

- Support of the DBT requirements through prevention of loss of nuclear material control and accounting for SSNM, as specified in 10 CFR 74.51(a), at Category I FCF licensees.

Protection against these DBTs has previously been identified by the Commission as necessary for adequate protection. As discussed in the regulatory basis document on the rulemaking for cyber security at FCFs (ADAMS Accession No. ML15355A466), Section 651 of the Energy Policy Act of 2005 directed the Commission to initiate a rulemaking to revise the DBTs set forth in 10 CFR 73.1. The Commission further directed consideration of, at a minimum, 12 factors when developing the DBT rule, specifically including a potential cyber threat. In 2007, in response to this direction, the Commission promulgated a rulemaking entitled, "Design Basis Threat" (72 *Federal Register* [FR] 12705), revising 10 CFR 73.1 to explicitly include a cyber security threat as an element of the DBTs necessary for adequate protection.

The Commission determined that a backfit analysis was not required for the DBT rule, pursuant to the exceptions in 10 CFR 50.109(a)(4)(iii) and 10 CFR 70.76(a)(4)(iv) for regulatory actions related to adequate protection. Specifically, the Commission stated in 72 FR 12705 that, "the Commission further finds that the final rule would redefine the security requirements stated in existing NRC regulations, and is necessary to ensure that the public health and safety and common defense and security are adequately protected in the current, post-September 11, 2001 environment." Accordingly, the DBT rule reflected the Commission's view that Category I FCF licensees must defend against a cyber attack in order to ensure adequate protection.

The current DBT cyber security requirements in 10 CFR 73.1, 73.45, "Performance capabilities for fixed site physical protection systems," and 73.46, "Fixed site physical protection systems, subsystems, components, and procedures," and related guidance in Regulatory Guide 5.70, "Guidance for the Application of the Theft and Diversion Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.45 and 73.46" (which is not publicly available), do not provide specific strategies or measures for FCF licensees to employ for protection against a cyber attack or to prevent a consequence of concern. These documents also lack specific performance criteria for FCF licensees to measure against. Consequently, licensees have implemented a broad range of cyber security initiatives that vary between facilities and lack enforceability. The current regulatory structure is not conducive for ensuring implementation of an effective cyber security program to provide for protection against the cyber security elements of the DBTs, as required for adequate protection.

The proposed rule for cyber security at FCFs would provide the program elements necessary to protect against the cyber security elements of the DBTs and are necessary to ensure that the public health and safety and common defense and security are adequately protected in the evolving threat environment.

III.3 Proposed classified information requirements necessary for adequate protection

FCF licensees that possess classified information are subject to specific requirements for its protection. All Category I FCF licensees and the Category III FCF licensee with classified information (e.g., enrichment facilities) would be impacted. As discussed in Section I.3 of this backfit analysis, current NRC regulations do not contain specific cyber security requirements to prevent the following security and safeguards event:

- Loss or unauthorized disclosure of classified information, as specified in 10 CFR Part 95, at FCFs in possession of classified information.

FCF licensees are required by 10 CFR Part 95 to prevent unauthorized access to classified information and matter. The compromise, due to a cyber attack, of a function needed to prevent loss or unauthorized disclosure of classified information is a consequence of concern in the proposed 10 CFR 73.53. Preventing this consequence of concern is necessary for adequate protection, consistent with Executive Order 13526, the Energy Reorganization Act of 1974, and 10 CFR Part 95.

In Executive Order 13526, Sec. 1.4, the President directed that, "classified information [be] used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection." Classified information includes both NSI and RD. Category I FCF licensees possess NSI information associated with "scientific, technological, or economic matters relating to the national security," "United States Government programs for safeguarding nuclear materials or facilities," or "the development, production, or use of weapons of mass destruction." Unauthorized disclosure of NSI, depending on its security level (i.e., Confidential, Secret, and Top Secret), can cause serious damage to the national security of the United States. In addition, RD as defined in the AEA, "means all data concerning: (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 142." Category I FCF licensees and Category III FCF licensees with classified information may possess RD (e.g., classified information concerning uranium enrichment technology that could have dual-use applications). These licensees must ensure that digital assets associated with the protection and physical security of NSI and RD information are adequately protected, consistent with Executive Order 13526, to prevent serious damage to the national security of the United States.

In addition, the AEA authorizes the NRC to prescribe such regulations or orders as it may deem necessary to protect RD received by any person in connection with any activity authorized pursuant to this Act (AEA Section 161(i)). Since the functions of digital assets can provide for both information security (e.g., records, information systems, and access control) and physical security (e.g., badge readers, cameras, and locks), these assets must be protected from a cyber attack that could result in a consequence of concern. Consequently, and as a direct extension of licensee obligations under 10 CFR Part 95 and other requirements, the proposed rule defines one of the consequences of concern as a compromise, as a result of a cyber attack, of a function needed to prevent loss or unauthorized disclosure of classified information. A cyber security program, consistent with the requirements in the proposed rule, is necessary to ensure that this consequence of concern does not occur. Therefore, for licensees with classified material, the cyber security program is necessary to ensure that

the common defense and security are adequately protected in the current, evolving threat environment.

The NRC requirements for protection of classified information and matter (i.e., NSI and RD) are defined in 10 CFR Part 95. The issuance of that regulation did not require backfit considerations to be addressed when the rule was first issued in FR notice (FRN) 45 FR 14476-14493, March 5, 1980, because the backfit regulations were not in place at that time. However, backfitting was addressed during a subsequent revision of the regulations in 62 FR 17683-17698, April 11, 1997. These regulations, including requirements to protect classified information and matter, were enacted under the backfit exception in 10 CFR 50.109(a)(4)(iii), "[t]hat the regulatory action involves defining or redefining what level of protection to the public health and safety or common defense and security should be regarded as adequate." As discussed above, this is consistent with the determination that the protection of classified information is necessary to ensure that the common defense and security are adequately protected.

The requirements defined in the proposed 10 CFR 73.53 would provide for a cyber security program that is necessary to prevent the latent security consequence of concern, due to a cyber attack, thereby ensuring adequate protection. As such, the proposed 10 CFR 73.53 is consistent with Executive Order 13526, the statutory requirements of the AEA and existing NRC regulations in 10 CFR Part 95.

III.4 Sections of the proposed rule required for adequate protection

Each provision of the cyber security program is necessary to ensure a cyber attack does not result in a consequence of concern. The proposed rule requires protection against these consequences of concern through a number of requirements in 10 CFR 73.53, including provisions regarding:

- performance objectives – 10 CFR 73.53(b);
- Cyber Security Team – 10 CFR 73.53(d)(1);
- cyber security controls – 10 CFR 73.53(d)(2), (5)(i), and (6);
- identification of VDAs – 10 CFR 73.53(d)(3)-(4);
- protection of VDAs – 10 CFR 73.53(d)(5)(ii);
- cyber security plan – 10 CFR 73.53(e);
- configuration management – 10 CFR 73.53(f); and
- periodic program reviews – 10 CFR 73.53(g).

Additional information on each of these proposed requirements is provided in Section I.4 of this backfit analysis. For each provision, a discussion is provided below on the how the requirement is necessary for adequate protection for the classes of licensees noted above.

III.4.1 Performance objectives – 10 CFR 73.53(b)

The establishment of performance objectives is a necessary element of a cyber security program, as described in this sub-section. The program is needed to prevent the latent DBT and latent security (i.e., safeguarding classified information) consequences of concern. Therefore, meeting the performance objectives to detect, protect against, and respond to a cyber attack is necessary for adequate protection.

Licensees must be able to detect cyber attacks in order to defend against them. Detection requires the licensee to have an understanding of the facility's cyber security activities, the potential attack pathways, and knowledge of normal and abnormal cyber activity. The detection objective also requires an ability to test assets for vulnerabilities, to conduct analysis to identify compromises, and recognize potential problems.

Licensees must be able to protect against cyber attacks capable of causing a consequence of concern. Protections require licensees to prevent unauthorized access to their assets. The protection objective entails the creation of a cyber security program to identify the potential attack pathways, addresses controls to prevent unauthorized access, and protects against a consequence of concern through intervention. Protection is an ongoing objective conducted throughout the life cycle of the facility.

In addition to taking reasonable measures to prevent cyber attacks from causing a consequence of concern, effective and timely response is a necessary performance objective. A response capability allows for VDAs under potential or actual threat of cyber attack to be placed in a safe condition to limit the extent of potential compromise. An adequate response also allows FCF licensees to preserve information about the nature of the attack. This objective requires that licensees have a trained and qualified staff capable of taking corrective actions in response to identified vulnerabilities or threats. This is also part of the Cyber Security Team requirement, which is discussed in the next subsection. The response objective would require cyber security measures to be designed with redundancies and fail-safes, when feasible, to allow intervention to prevent a cyber attack from resulting in a consequence of concern. This provides the licensee with the ability to intervene, such as placing the compromised asset into a safe condition to limit the extent of the compromise or vulnerability. A necessary part of the response also involves FCF licensees preserving, where possible, all evidence of the attack for investigation.

The performance objectives of detection, protection, and response are necessary because they establish the basic expectations for a minimally effective cyber security program. The various components of the cyber security program are implemented to meet these performance objectives. Therefore, these performance objectives require protection against the DBTs and the compromise of classified information consequences of concern. As a result, the performance objectives are necessary for adequate protection of the health and safety of the public and are in accord with the common defense and security.

III.4.2 The Cyber Security Team – 10 CFR 73.53(d)(1)

As noted above, the creation of the Cyber Security Team, as described in this sub-section, is a necessary element of the cyber security program. The program is needed to prevent the latent DBT and latent security (i.e., safeguard classified information) consequences of concern.

A necessary component of an effective cyber security program is the establishment of a Cyber Security Team that is adequately structured, staffed, trained, qualified, and equipped to protect against cyber attacks that could result in a consequence of concern. A management structure for the Cyber Security Team must be in place to provide sufficient resources and authority to meet the performance objectives. The team members must include individuals with cyber security expertise, knowledge of safety, security, and safeguards systems, as well as knowledge of facility operations in order to ensure that the cyber security program is effective and comprehensive. The individuals on the team need to have appropriate training and qualifications to ensure they are knowledgeable of current threats, facility vulnerabilities, and understand how to implement solutions. Members of the team also need to be able to respond in a timely manner to prevent a consequence of concern. The team must be equipped with the cyber security tools (e.g., software and services) to protect the facility's safety, security, and safeguards systems.

The Cyber Security Team is necessary because qualified individuals must implement the cyber security program to meet the performance objectives. Therefore, the Cyber Security Team is necessary for protection against the DBTs and the compromise of classified information consequences of concern. As a result, the Cyber Security Team is necessary for adequate protection of the health and safety of the public and is in accord with the common defense and security.

III.4.3 Developing and maintaining cyber security controls – 10 CFR 73.53(d)(2), (5)(i), and (6)

The development and application of cyber security controls is a necessary element of a minimally effective cyber security program, as described in this sub-section. The program, and these controls, are needed to prevent the latent DBT and latent security (i.e., safeguard classified information) consequences of concern.

Cyber security controls are performance specifications used to inform the measures taken to detect, protect against, or respond to a cyber attack capable of causing a consequence of concern. These cyber security controls are specific to each of the applicable types of consequences of concern. The measures consist of the actions to implement the controls effectively including: assigning values to internal parameters specific to the VDAs; documenting the procedures for applying the controls; and enacting the controls as part of routine operations. Establishing and maintaining cyber security controls is necessary to effectively protect VDAs.

The consequences of concern (e.g., latent DBT and latent security) require different levels of controls and control parameters to protect different VDAs. Once identified, the controls are documented, as commitments, in the cyber security plan. The licensee addresses the controls by taking specific measures to ensure effective protection of VDAs. When the measures become degraded, temporary compensatory measures are

enacted to maintain an equivalent level of protection. Thus, the proposed rule would ensure that licensees identify and commit to the controls necessary to protect the facility's VDAs, thus preventing a consequence of concern. Therefore, cyber security controls are required for protection against the DBTs and the compromise of classified information consequences of concern. As a result, the cyber security controls are necessary for adequate protection of the health and safety of the public and are in accord with the common defense and security.

III.4.4 Completing the identification of VDAs – 10 CFR 73.53(d)(3)-(4)

The analysis to identify VDAs is also a necessary element of the cyber security program, as described in this sub-section. The cyber security program is needed to prevent the latent DBT and latent security (i.e., safeguard classified information) consequences of concern.

The analysis of digital assets enables licensees to determine what devices and related support systems (e.g., power supply, calibration, and heating, ventilation, and air conditioning) are vulnerable to a cyber attack to ensure they are properly protected. This allows the Cyber Security Team to distinguish between digital assets that do not require additional protection and those that do (i.e., VDAs). The identification of VDAs ensures that licensee resources are focused on preventing consequences of concern through protection of the appropriate digital assets. The analysis creates a baseline set of devices that the licensee monitors to detect and respond to cyber attacks, and to track for its configuration management system.

The analysis to identify VDAs is a necessary part of the cyber security program because FCF licensees must determine and document which associated support systems require protection. Therefore, the analysis to identify VDAs is required for protection against the DBTs and the compromise of classified information consequences of concern. As a result, the analysis to identify VDAs is necessary for adequate protection of the health and safety of the public and is in accord with the common defense and security.

III.4.5 Implementing the measures to ensure the protection of VDAs – 10 CFR 73.53(d)(5)(ii)

Ensuring the protection of VDAs by implementing the measures to address cyber security controls is a necessary element of the cyber security program, as described in this sub-section. The cyber security program is needed to prevent the latent DBT and latent security (i.e., safeguard classified information) consequences of concern.

Implementation of those measures consists of providing equipment and administrative actions to meet the performance specifications of the controls for VDAs. These are documented in the implementing procedures for applying controls to VDAs. The implementing procedures contain the specific parameters and timeframes licensees must follow to successfully protect the VDA. The implementing procedures describe: how the controls function and should be installed and maintained; training or operating requirements; and any other appropriate considerations for their effective application. The implementing procedures also provide a written record to confirm that the controls meet the program objectives.

Implementing the measures taken to address cyber security controls are a necessary part of the cyber security program because those measures describe how to apply the cyber security specified by the controls. Therefore, implementation of those measures is required for protection against the DBTs and the compromise of classified information consequences of concern. As a result, the implementation of those measures is necessary for adequate protection of the health and safety of the public and is in accord with the common defense and security.

III.4.6 Creating and maintaining a cyber security plan – 10 CFR 73.53(e)

The cyber security plan is a necessary element of the cyber security program, as described in this sub-section. The cyber security program is needed to prevent the latent DBT and latent security (i.e., safeguard classified information) consequences of concern.

The cyber security plan contains the specific licensing commitments for a FCF licensee's cyber security program. The plan is necessary for FCF licensees to document that the various components of the cyber security program are comprehensive, complete, and meet the performance objectives prior to program implementation. The cyber security plan must contain a description of the cyber security program and associated controls, and it will be reviewed and approved by the NRC. Once approved, the plan and the cyber security program become enforceable requirements

The cyber security plan ensures the cyber security program is acceptable, and as such, it becomes part of the licensing basis. The cyber security plan is required for protection against the DBTs and the compromise of classified information consequences of concern. As a result, the cyber security plan is necessary for adequate protection of the health and safety of the public and is in accord with the common defense and security.

III.4.7 Conducting configuration management – 10 CFR 73.53(f)

Configuration management is a necessary element of the cyber security program. The cyber security program is needed to prevent the latent DBT and latent security (i.e., safeguard classified information) consequences of concern.

Configuration management ensures that the cyber security program remains a reliable and effective program for preventing a compromise of VDAs due to a cyber attack, that could result in a consequence of concern. Both the cyber security threat environment and operational processes of FCF licensees are expected to change over time. Changes in the threat environment may result in licensees identifying new VDAs, new controls, or other modifications to protect against current threat vectors. As a result, a configuration management system is needed to evaluate these dynamic elements and ensure resultant changes are implemented consistent with the change management requirements proposed in 10 CFR 40.35(g) and 70.32(f). Licensees must stay cognizant of the changing threat environment and maintain assets up-to-date (e.g., routine software updates to maintain appropriate protection). These updates may require pre-testing in a controlled environment prior to facility wide implementation.

Configuration management is necessary to evaluate, prior to implementation, the impacts of proposed changes to FCF safety, security, and safeguards systems. Unless analyzed in advance, FCF changes may have adverse impacts on VDAs, related

support systems, and controls. Configuration management provides for documentation to track facility changes and includes TCMs to provide interim protection until permanent controls are in place to prevent the consequences of concern.

The configuration management system is a necessary part of the cyber security program because it ensures protection of VDAs and related support systems, as well as ensures that controls remain reliable and effective. Therefore, the configuration management system is required for protection against the DBTs and the compromise of classified information consequences of concern. As a result, the configuration management system is necessary for adequate protection of the health and safety of the public and is in accord with the common defense and security.

III.4.8 Completing periodic program reviews – 10 CFR 73.53(g)

Periodic program reviews are a necessary element of the cyber security program. The cyber security program is needed to prevent the latent DBT and latent security (i.e., safeguard classified information) consequences of concern.

Periodic review of the entire cyber security program is necessary to ensure that program elements, including VDAs, controls, and procedures, continue to be appropriately identified, documented, and implemented. This effort is needed to identify discrepancies between the cyber security plan and facility practices; this facilitates modifications to the plan, or facility practices, as appropriate. It also provides for an audit that can reveal overlooked vulnerabilities and facilitate corrective action.

The periodic review is a necessary part of the cyber security program because it provides for an audit to evaluate the effectiveness of the cyber security program to meet performance objectives. Therefore, the periodic review of the cyber security program is required for protection against the DBTs and the compromise of classified information consequences of concern. As a result, the periodic review of the cyber security program is necessary for adequate protection of the health and safety of the public and is in accord with the common defense and security.

III.5 Conclusion

The proposed rule requirements for protection against the DBTs and the compromise of classified information consequences of concern are necessary to ensure that the common defense and security are adequately protected. The programmatic elements discussed above associated with protecting against those consequences of concern therefore are not subject to a backfit analysis demonstrating a substantial increase in overall protection and cost justification. Those program elements and associated consequences of concern are analyzed below in Sections IV and V.

IV. BACKFIT ANALYSIS: SUBSTANTIAL INCREASE IN OVERALL PROTECTION

The NRC staff has identified certain provisions of the proposed rule that qualify as a backfit and that are not subject to any exceptions to a backfit analysis in 10 CFR 70.76. Therefore, a backfit analysis must be performed for these provisions in accordance with 10 CFR 70.76(a)(3). The first part of this backfit analysis is to determine whether there is a, "substantial increase in the overall protection of the public health and safety or the common defense and security to be derived from the backfit."

The provisions in the proposed rule that are subject to a backfit analysis are the cyber security requirements associated with protecting against the safety-related consequences of concern found in 10 CFR 73.53(c)(3) and 10 CFR 73.53(c)(4)(i)-(iii). Both include the following exposure thresholds for radiological and chemical releases to any individual (i.e., public and occupational exposures):

- A radiological exposure of 25 rem or greater for any individual;
- An intake of 30 mg or greater of uranium in soluble form for any individual outside the controlled area; or
- An acute chemical exposure that could lead to irreversible or other serious, long-lasting health effects for any individual.

The exposure thresholds in 10 CFR 73.53(c)(3) are designated as active safety consequences of concern when they can be directly caused by a cyber attack. The same exposure thresholds are also in 10 CFR 73.53(c)(4)(i)-(iii), where they are designated as latent safety consequences of concern. A latent consequence of concern involves the compromise, as a result of a cyber attack, of a function needed to prevent exposures at or above these thresholds that are caused by a separate initiating event.

As described in Section III of this backfit analysis, the protection against the DBTs and the compromise of classified information consequences of concern are derived from existing regulatory requirements which are necessary for adequate protection. The proposed requirements for preventing active safety or latent safety consequences of concern by a cyber attack are not required for adequate protection. Protection against these safety consequences of concern also derive from existing requirements. As described in this section, the NRC staff finds that the implementation of these proposed requirements would provide a substantial increase in overall protection.

FCF licensees are required by 10 CFR 70.23(a)(3) to ensure that licensed operations are conducted safely. This includes the safe operation of digital assets. Exploitation of vulnerabilities in digital assets, as demonstrated by the real world examples presented in the Draft RA, Appendix B, can cause a consequence of concern (i.e., the active consequence of concern), or compromise the function of safety or security systems needed to prevent a consequence of concern (i.e., the latent consequence of concern). Licensees must ensure that all safety, security, and safeguards systems, including those having digital assets, facilitate the regulatory requirement to safely operate the facility.

While the consequences are potentially significant, FCF licensees are not currently required to consider potential radiological or chemical consequences of cyber attacks. The proposed rule would require protection from a cyber attack capable of resulting in an

active safety or latent safety consequence of concern.

Implementation of the ISA requirements in 10 CFR Part 70 Subpart H, "Additional Requirements for Certain Licensees Authorized to Possess a Critical Mass of Special Nuclear Material," requires certain licensees to identify IROFS to prevent or mitigate high and intermediate consequence safety events. These provisions require that FCF licensees ensure that IROFS remain available and reliable, however the provisions are silent in regards to a cyber attack. Cyber attacks have the potential to compromise the function of a safety system such as IROFS, potentially resulting in a latent consequence of concern. The cyber security program requirements in the proposed rule would ensure that those digital assets used for safe operations, like IROFS, remain available and reliable. Cyber attacks could also compromise such safety systems and cause an active consequence of concern. Implementation of the proposed rule would protect against safety consequences of concern, and as further discussed in the Draft RA, Sections 4.2.6, "Public Health (Accident)," and 4.2.8, "Occupational Health (Accident)," would significantly reduce the risk of such an event occurring, and therefore provides a substantial increase in overall protection.

IV.1 Finding of a substantial increase in overall protection of public health and safety

NUREG-1409 describes a significant increase in the overall protection of public health and safety as one that is important or significant in a large amount, extent, or degree. As further discussed in Section V, "Backfit Analysis: Cost Justification" and the assumptions therein, the benefits associated with the implementation of the proposed rule are reflected in the following table:

Table IV-1 Summary of averted cost per single event

Event	Cost description	Minimum averted cost	Maximum averted cost
Radiological exposure	Injury/death	$132,500	$90,000,000
	Clean-up/decon	$6,400	$7,200,000
	Total	$138,900	$97,200,000
Intake of 30 mg or greater of uranium in soluble form outside the controlled area	Injury/death	$397,500	$56,445,000
	Clean-up/decon	$6,400	$2,216,630
	Total	$403,900	$58,661,630
Acute chemical exposure	Injury/death	$423,000	$883,368,000
	Clean-up/decon	$6,400	$2,216,630
	Total[1]	$429,400	$885,584,630

The NRC staff concluded that the averted cost of a single event associated with a safety consequence of concern is, at a minimum, on the order of hundreds of thousands of dollars, with mid-range values in the tens of millions of dollars, and maximum values in the hundreds of millions of dollars. Section V.5, "Benefits," of this backfit analysis further demonstrates that effective protection against these events would constitute a significant

[1] The totals are the minimum and maximum costs for the direct harm due to a single event, and do not include costs to respond to the event, support NRC investigation, maintenance of safe facility conditions during response and recovery, or implementation of potential subsequent requirements to ensure there is no recurrence.

increase in overall protection of public health and safety.

IV.2 Section-by-section analysis for substantial increase in overall protection

Why are these cyber security requirements needed for the substantial increase in overall protection?

The NRC staff has identified the need for cyber security regulations for preventing the active safety or latent safety consequences of concern by a cyber attack based on the developing threat environment and observed vulnerabilities in the cyber security programs at FCFs. The developing threat environment is discussed further in the Draft RA, Appendix B. Recent cyber attacks outside of the nuclear industry have resulted in physical impacts. These cyber attacks utilized methods that could compromise comparable functions and assets at FCFs. In addition, the staff has observed a wide range of voluntary cyber security measures at FCFs of varying effectiveness. Under the current regulations, FCF licensees are not required to specifically analyze their facilities and identify those VDAs whose compromise could lead to significant consequences, such as a safety consequence of concern. Without the cyber security program requirements in the proposed rule, FCF licensees are more susceptible to cyber attacks that could compromise a VDA and result in a safety consequence of concern.

IV.3 Section-by-section analysis

Similar to the adequate protection discussion above for the DBT and classified information consequences of concern, the different provisions of the proposed cyber security rule would provide the necessary program elements to effectively protect against a safety consequence of concern, and thereby provide a substantial increase in overall protection. These requirements include:

- the performance objectives – 10 CFR 73.53(b);
- the Cyber Security Team – 10 CFR 73.53(d)(1);
- cyber security controls – 10 CFR 73.53(d)(2), (5)(i), and (6);
- identification of VDAs – 10 CFR 73.53(d)(3)-(4);
- protection of VDAs – 10 CFR 73.53(d)(5)(ii);
- cyber security plan – 10 CFR 73.53(e);
- configuration management – 10 CFR 73.53(f); and
- periodic program reviews – 10 CFR 73.53(g).

As previously noted, the reporting and records retention requirements (i.e., 10 CFR 73.53(h) and 10 CFR 73.53(i), respectively) are not subject to backfit analysis.

Additional information on all of these proposed requirements is provided above in Section I.4. For each provision, a discussion is provided below on how the requirement provides a substantial increase in overall protection through an effective cyber security program.

IV.3.1 Meeting the performance objectives – 10 CFR 73.53(b)

The establishment of performance objectives is a necessary element of the cyber security program, as described in this sub-section. The program is needed to protect against the safety consequences of concern. Therefore, meeting the performance objectives to detect, protect against, and respond to a cyber attack provides a substantial increase in overall protection.

The performance objectives of detection, protection, and response are necessary for a cyber security program to prevent the safety-related consequences of concern. The proposed rule would require that FCF licensees establish and maintain a cyber security program with clear objectives to defend against a cyber attack. These performance objectives are located in proposed 10 CFR 73.53(b) as described in Section I.4 of this backfit analysis and are further described in DG-5062, "Cyber Security Programs for Nuclear Fuel Cycle Facilities" (ADAMS Accession No. ML16319A320).

An acceptable detection process allows for identification of abnormal activity in a timely manner so that the licensee can evaluate the potential impacts, and implement compensatory measures or take other responsive action, as necessary. Detection also provides the licensee information on the type of attacks occurring so the response can be effective. Detection provides awareness of the ongoing cyber security threat and supports the effectiveness of the cyber security program.

Protection involves conducting an analysis to determine which digital assets are VDAs and applying appropriate measures, as discussed below. This ensures that assets whose compromise could cause a safety consequence of concern are protected. Protection also involves using proper configuration management when making facility modifications and is therefore an ongoing objective that must be satisfied throughout the life of the facility.

Effective and timely response to a cyber attack is likewise critical to an effective cyber security program. A response capability allows for VDAs under potential or actual threat of cyber attack to be placed in a safe condition to limit the extent of the compromise. An adequate response also allows FCF licensees to preserve, where possible, all evidence of the attack for investigation.

The performance objectives of detection, protection, and response establish the basic goals for an effective cyber security program. As such, they are a necessary element for a cyber security program to protect against a safety consequence of concern. Therefore, the performance objectives in the proposed rule provide a substantial increase in overall protection.

IV.3.2 Establishing and maintaining the Cyber Security Team – 10 CFR 73.53(d)(1)

The creation of a Cyber Security Team is a necessary element of the cyber security program, as described in this sub-section. The program is needed to protect against the safety consequences of concern. Therefore, establishing and maintaining a Cyber Security Team provides a substantial increase in overall protection.

An adequately structured, staffed, trained, qualified, and equipped Cyber Security Team is a basic requirement for the effective implementation and management of a cyber

security program to meets the performance objectives. Appropriately skilled personnel can identify VDAs and ways to protect them from cyber attacks. They can also be available to respond to and analyze an attack. Dedicated personnel can efficiently and effectively address cyber security issues associated with a consequence of concern.

The National Institute for Standards and Technology (NIST), the authoritative source for cyber security standards and practices for the Federal Government, recommends a Cyber Security Team for organizations using computer technology. Digital assets at FCFs, including some that also impact IROFS, would be susceptible to cyber attacks without an appropriate cyber security program overseen by qualified personnel, as further discussed in the Draft RA, Appendix B. The Cyber Security Team would conduct an analysis and implement controls for these digital assets to ensure protection of the VDAs from a consequence of concern.

The Cyber Security Team develops, implements, and maintains the cyber security program. As such, the team is a necessary element for the program to protect against a safety consequence of concern. Therefore, the Cyber Security Team requirements for the cyber security program provide a substantial increase in overall protection.

IV.3.3 Developing and maintaining cyber security controls – 10 CFR 73.53(d)(2), (5)(i), and (6)

The application of cyber security controls is a necessary element of the cyber security program, as described in this sub-section. The program is needed to protect against the safety consequences of concern. Therefore, developing and maintaining cyber security controls provides a substantial increase in overall protection.

Cyber security controls are performance specifications used to inform the measures taken to detect, protect against, or respond to a cyber attack capable of causing a consequence of concern. Each control is a performance measure (e.g., derived from NIST's Special Publication "Security and Privacy Controls for Federal Information Systems and Organizations" (NIST SP 800-53, Revision 4)), which can be implemented by the licensee for the protection of a VDA against a given threat or possible vulnerability. These controls are designed to address specific areas of vulnerability that can be exploited if not protected.

These controls provide the measures necessary to establish whether or not a VDA is effectively protected against threats. The controls provide the performance measures to determine if cyber security protections are effective. Similar concepts inform cyber security protections for power reactors.

The controls provide flexibility for FCF licensees to protect the affected VDAs. The comprehensiveness of the controls is graded based on the associated consequence of concern. In addition, individual controls can be tailored based upon the facility's needs and the condition of the VDAs. This flexibility ensures that licensee resources are used effectively.

The cyber security controls provide the performance measures implemented through the cyber security program to protect VDAs from a compromise leading to a safety consequence of concern. Therefore, the cyber security controls are necessary for the proposed rule to provide a substantial increase in overall protection.

IV.3.4 Completing the identification of VDAs – 10 CFR 73.53(d)(3)-(4)

The analysis to identify VDAs is a necessary element of the cyber security program, as described in this sub-section. The program is needed to protect against the safety consequences of concern. Therefore, identification of VDAs provides a substantial increase in overall protection.

The proper identification of VDAs is necessary to determine which VDAs must be protected from cyber attacks. This process gives each FCF licensee the opportunity to evaluate the facility's digital assets and determine whether or not they are associated with a safety consequence of concern. The evaluation includes an assessment of the digital asset's dependence on support systems which may also require protection to prevent a compromise. The proposed rule would allow FCF licensees to identify alternate means for protection against the consequences of concern, which would eliminate the need to apply controls to digital assets.

In addition, a facility-wide analysis allows for identification of any commonalities that exist among the various VDAs (e.g. devices that exist on the same network, equipment that is of the same type or configuration), which allows for the application of common controls to limit the overall burden on FCF licensees. The identification of VDAs improves the detection of, and response to, cyber attacks by enabling licensees to focus their efforts on those assets that require protection.

The identification of VDAs ensures FCF licensees are aware of the assets that need to be protected by the cyber security program to prevent a compromise leading to a safety consequence of concern. Therefore, the identification of VDAs is necessary for the proposed rule to provide a substantial increase in overall protection.

IV.3.5 Implementing the measures to ensure the protection of VDAs – 10 CFR 73.53(d)(5)(ii)

Implementing the measures for the protection of VDAs is a necessary element of the cyber security program, as described in this sub-section. The program is needed to protect against the safety consequences of concern. Therefore, implementing the measures for the protection of VDAs provides a substantial increase in overall protection.

The implementation of measures for the protection of VDAs involves the physical or administrative changes FCF licensees undertake. These could include installing new equipment, computer programming, or changing existing procedures. The protections consist of applying controls identified in the cyber security plan and assigning control parameters to the specific VDAs. Prior to implementation, these protective measures would be tested under controlled conditions to ensure they function as expected. Procedures would describe: how the measures function; how they would be installed or used; what training or operating requirements apply; and any other relevant considerations.

Through procedures, FCF licensees will control the steps for implementation of measures to ensure that they have been properly applied and are documented. This provides traceability and helps confirm that the program objectives are met.

The implementation of the measures and associated procedures in the cyber security program protects VDAs from a cyber attack that could cause a compromise leading to a safety consequence of concern. Therefore, implementing the measures for the protection of VDAs is necessary for the proposed rule to provide a substantial increase in overall protection.

IV.3.6 Creating and maintaining a cyber security plan – 10 CFR 73.53(e)

The cyber security plan is a necessary element of the cyber security program, as described in this sub-section. The program is needed to protect against the safety consequences of concern. Therefore, creating and maintaining a cyber security plan provides a substantial increase in overall protection.

A cyber security plan documents the commitments of a FCF licensee regarding its cyber security program, including how the licensee will: satisfy the requirements of the proposed rule; manage its cyber security program; and provide incident response for a cyber attack capable of causing a safety consequence of concern. The plan would describe how the program would be implemented, what controls would be used to protect VDAs, and how performance would be measured. This document would describe the necessary protective measures, detection capabilities, and response actions.

In addition, the proposed requirement for FCF licensees to develop and submit for approval a cyber security plan provides assurance to the NRC that the program complies with NRC regulations. The plan is included in the license as part of the licensing basis. The NRC staff inspect and confirm the program is implemented consistent with commitments in the plan. NRC review and approval of the cyber security plan also ensures the FCF licensee's cyber security program complies with program requirements.

The cyber security plan documents the various elements of the cyber security program implemented to prevent a compromise of a VDA leading to a safety consequence of concern. It also provides for program control, and clarity in expectations for the licensee and the NRC. The cyber security plan is therefore necessary for the cyber security program, and provides a substantial increase in overall protection.

IV.3.7 Conducting configuration management on facility activities as well as existing VDAs – 10 CFR 73.53(f)

Configuration management is a necessary element of the cyber security program. The program is needed to protect against the safety consequences of concern. Therefore, conducting configuration management on FCF activities as well as existing VDAs provides a substantial increase in overall protection.

Configuration management is necessary to ensure the cyber security program remains effective over the lifetime of the facility. Since the cyber threat environment changes over time, FCF licensees need to manage their cyber security program, and make adjustments as necessary for the continuous protection of VDAs. Additionally, FCFs, like any industrial facility, are modified, upgraded, and change over time. Changes to the facility can be a significant pathway for the introduction of new cyber security

vulnerabilities. Thus, FCF licensees need to review the impacts of proposed facility changes on cyber security. The configuration management system provides for monitoring and awareness of facility changes to protect against threats to safety, security, and safeguards systems. Through this program, the licensee identifies changes to the facility potentially associated with the safety consequences of concern. Therefore, the configuration management system is necessary for an effective cyber security program, and provides a substantial increase in overall protection.

IV.3.8 Completing periodic program reviews – 10 CFR 73.53(g)

Periodic program reviews are a necessary element of the cyber security program. The program reviews are needed to protect against safety consequences of concern. Therefore, conducting periodic cyber security program reviews provides a substantial increase in overall protection.

A periodic review of the cyber security program is essential to ensure that cyber security protections remain effective over time. This periodic review provides for an audit of the effectiveness of the various cyber security program elements in order to meet the program objectives. Through periodic program reviews, the licensee assesses the effectiveness of the cyber security program, including the purpose, scope, roles, responsibilities, requirements, and management.

Through periodic program reviews, the licensee ensures that the performance measures, established through cyber security controls and associated implementing procedures, are developed, monitored, and maintained appropriately. Alternate means and defensive architecture are also reviewed periodically to ensure they continue to protect against safety consequences of concern. The periodic program reviews also include an evaluation of the effectiveness of configuration management.

Through periodic program reviews, the licensee identifies potential weaknesses and allows the licensee to take appropriate corrective action to prevent a compromise in cyber security protections from leading to a safety consequence of concern. Therefore, periodic cyber security program reviews are necessary for an effective cyber security program and provide a substantial increase in overall protection.

IV.4 Conclusion

The proposed rule provides for a cyber security program that can protect against the safety consequences of concern in 10 CFR 73.53(c)(3) and 10 CFR 73.53(c)(4)(i)-(iii). The individual elements of this program, described above, are necessary for an effective cyber security program. The NRC staff therefore concludes, consistent with 10 CFR 70.76(a)(3), that a cyber security program with each of the elements described above, provides a substantial increase in overall protection of the public health and safety by protecting against the safety consequences of concern, as further described in the FRN for the proposed rule (ADAMS Accession No. ML17018A220), in Section IV.K entitled, "How are the consequences of concern used in the proposed rule?" This protection against consequences of concern is needed in light of the evolving cyber security threat, as further discussed in the Draft RA, Appendix B. Having found that the proposed requirements provide a substantial increase in safety, consistent with 10 CFR 70.76(a)(3), the staff next considers whether the proposed requirements are cost-justified.

V. BACKFIT ANALYSIS: COST JUSTIFICATION

As discussed in Section IV, those elements of the proposed rule that constitute a backfit on protected entities were found to provide a substantial increase in the overall protection of public health and safety. The NRC staff now considers whether the proposed requirements are cost justified, as described in 10 CFR 70.76(a)(3). The backfit analysis includes monetary, as well as qualitative and uncertainty cost considerations. The analysis of benefits also includes qualitative considerations which the staff cannot estimate numerically because the number and severity of future cyber attacks cannot be calculated meaningfully. The staff finds that the proposed requirements associated with the safety consequences of concern are cost-justified in light of the averted costs from a consequence of concern, given monetary, uncertainty, and qualitative considerations.

V.1 Costs

This section of the backfit analysis identifies the costs associated with the provisions of the proposed rule, identified in Section IV, pertaining to the safety consequences of concern. The costs for the provisions of the proposed rule required for adequate protection are excluded from this consideration of costs (they are considered in the Draft RA). For Category I FCF licensees and Category III FCF licensees with classified information, only the additional costs associated with the safety consequences of concern are considered. For Category III FCF licensees that do not have classified information, all the costs associated with the proposed rule are considered. These qualifiers resulted in the following cost assumptions drawn from Table I-3 as described in Section I.6, "Considerations of backfit for existing facilities":

- For Category I FCF licensees, 25 percent of the level of effort is estimated to be safety related;
- For Category III FCF licensees with classified information, 25 percent of the level of effort estimated to be safety related;
- For Category III FCF licensees without classified information, 100 percent of the effort is estimated to be safety related;
- For Category I FCF licensees and Category III FCF licensees with classified information, certain portions of the proposed rule (i.e., the performance objectives, the Cyber Security Team, cyber security plan, configuration management) are completely required for adequate protection; and
- For Category I FCF licensees and Category III FCF licensees with classified information, the costs of certain provisions of the proposed rule (i.e., identification of VDAs, protection of VDAs, and periodic program reviews) are partially required for adequate protection and partially considered here. The cost distribution for these program elements is based upon the overall distribution between elements necessary for adequate protection and those subject to the backfit analysis for that facility.

In the analysis below, the provisions of the proposed rule that are necessary for adequate protection are excluded from the cost justification. The provisions partially necessary for adequate protection and partially cost justified have the costs apportioned based on the percentages drawn from Table I-3 as described in Section I.6 of this backfit

analysis. The costs for each provision of the proposed rule are derived from the Draft RA. The analysis is divided between implementation and annual operational costs.

V.2 Implementation costs

The costs in this section account for procedural and administrative activities, equipment, labor, and materials required for implementation of the proposed rule at applicable FCFs. The proposed action would require licensees to make facility modifications and to revise their cyber security plans as well as complete other implementation activities.

V.2.1 Establishing the Cyber Security Team – 10 CFR 73.53(d)(1)

This activity would include hiring personnel, conducting training as necessary, and providing equipment so that team members can perform their duties. The industry costs for creating the Cyber Security Team are provided in the Draft RA, Section 4.2.1, "Industry Implementation," sub-section "Cyber Security Team." The estimated costs are $40,000 per FCF. The percentage of costs, identified in Table I-3 and described in Section I.6, associated with the substantial increase in overall protection are:

- 0 percent[2] of the costs for Category I FCF licensees (three facilities);
- 0 percent[2] of the costs for the Category III FCF licensee with classified information (one facility); and
- 100 percent of the costs for the Category III FCF licensees without classified information (three facilities).

Therefore, the total industry cost equals the cost of establishing the Cyber Security Team per facility multiplied by the number of facilities that need the team for a substantial increase in protection:

$$\frac{\$40{,}000}{\text{facility}} \times 3 \text{ facilities} = \$120{,}000$$

The industry cost of establishing the Cyber Security Team for the applicable facilities are estimated to be $120,000.

V.2.2 Creating a cyber security plan – 10 CFR 73.53(d)(2) and (6)

This activity would include documentation of a FCF licensee's cyber security program. The plan would be submitted to the NRC for review and approval prior to being included as a license condition. The industry costs for creating the cyber security plan are provided in the Draft RA, Section 4.2.1, "Industry Implementation," sub-section "Cyber Security Plan." The estimated costs are $48,494 per FCF. The percentage of costs, identified in Table I-3 and described in Section I.6, associated with the substantial increase in overall protection are:

- 0 percent[2] of the costs for Category I FCF licensees (three facilities);
- 0 percent[2] of the costs for the Category III FCF licensee with classified

[2] This means that the cost of this requirement is allocated fully for adequate protection, and that these costs are excepted from this backfit cost consideration.

information (one facility); and
- 100 percent of the costs for the Category III FCF licensees without classified information (three facilities).

Therefore, the total industry cost equals the cost of creating the cyber security plan per facility multiplied by the number of Category III licensees without classified information:

$$\frac{\$48,494}{\text{facility}} \times 3 \text{ facilities} = \$145,482$$

The industry cost of creating the cyber security plans for the applicable facilities are estimated to be $145,482.

V.2.3 Completing the identification of VDAs – 10 CFR 73.53(d)(3)-(4)

This activity would include identification of VDAs associated with the safety consequences of concern. This involves creating an inventory of digital assets that if compromised by a cyber attack would cause a consequence of concern and determining if those assets are VDAs. The industry costs for identification of VDAs are provided in the Draft RA, Section 4.2.1, "Industry Implementation," sub-section "Analysis of digital assets." The estimated costs are $148,500 per FCF. The percentage of costs, identified in Table I-3 and described in Section I.6, associated with the substantial increase in overall protection are:

- 25 percent of the costs for Category I FCF licensees (three facilities);
- 25 percent of the costs for the Category III FCF licensee with classified information (one facility); and
- 100 percent of the costs for the Category III FCF licensees without classified information (three facilities).

The total costs are calculated as follows:

$$\frac{\$148,500}{\text{facility}} \times \left(3 \text{ facilities}\left(\frac{25\%}{100\%}\right) + 1 \text{ facility}\left(\frac{25\%}{100\%}\right) + 3 \text{ facilities}\left(\frac{100\%}{100\%}\right)\right) = \$594,000$$

The industry costs for analyzing digital assets for the applicable facilities are estimated to be $594,000.

V.2.4 Developing cyber security controls – 10 CFR 73.53(d)(2), (5)(i), and (6)

This activity would include the creation and documentation of cyber security controls and specific performance characteristics. The industry costs for creating the cyber security controls are provided in the Draft RA, Section 4.2.1, "Industry Implementation," sub-section "Address cyber security controls and implementing procedures for application of cyber controls to VDAs." The estimated costs are $111,564 per FCF. The percentage of costs, identified in Table I-3 and described in Section I.6, associated with the substantial increase in overall protection are:

- 25 percent of the costs for Category I FCF licensees (three facilities);
- 25 percent of the costs for the Category III FCF licensee with classified information (one facility); and
- 100 percent of the costs for the Category III FCF licensees without classified information (three facilities).

The total costs are calculated as follows:

$$\frac{\$111,564}{\text{facility}} \times \left(3 \text{ facilities}\left(\frac{25\%}{100\%}\right) + 1 \text{ facility}\left(\frac{25\%}{100\%}\right) + 3 \text{ facilities}\left(\frac{100\%}{100\%}\right)\right) = \$446,256$$

The industry costs of developing the cyber security controls for the applicable facilities are estimated to be $446,256.

V.2.5 Implementing the measures to ensure the protection of VDAs – 10 CFR 73.53(d)(5)

This activity would include implementing and documenting the tasks to protect VDAs once identified. This may include facility changes, purchasing equipment, installing the equipment, training, and verifying that the proposed measures function. The industry costs for protection of VDAs are provided in the Draft RA, Section 4.2.1, "Industry Implementation," sub-section "Other industry implementation cost." The estimated costs are $197,000 per FCF. The percentage of costs, identified in Table I-3 and described in Section I.6, associated with the substantial increase in overall protection are:

- 25 percent of the costs for Category I FCF licensees (three facilities);
- 25 percent of the costs for the Category III FCF licensee with classified information (one facility); and
- 100 percent of the costs for the Category III FCF licensees without classified information (three facilities).

The total costs are calculated as follows:

$$\frac{\$197,000}{\text{facility}} \times \left(3 \text{ facilities}\left(\frac{25\%}{100\%}\right) + 1 \text{ facility}\left(\frac{25\%}{100\%}\right) + 3 \text{ facilities}\left(\frac{100\%}{100\%}\right)\right) = \$788,000$$

The industry costs for protection of VDAs for the applicable facilities are estimated to be $788,000.

V.3 Annual operational costs

FCF licensees would experience a number of annual operational costs associated with routine and recurring activities required by the proposed rule. The proposed rule would require licensees to conduct additional, ongoing cyber security activities beyond those accounted for in the implementation costs.

These annual operational costs are applicable over the remaining period of FCF operations, which is estimated to be an average term of 25 years from 2018. This estimate is based on the average license term for FCFs and the assumption that the

final rule could be issued as early as 2018. As a result, the average remaining life for currently licensed FCFs would be 25 years from the issuance date of the final rule. The costs used in this section are drawn from the undiscounted annual rate identified in Table 4-7 of the Draft RA. These annual rates are multiplied by 25 years to obtain total costs for the entire analysis period.

V.3.1 Completing periodic program reviews – 10 CFR 73.53(g)

FCF licensees would be required to conduct a regular review of the cyber security program. This would entail reviewing audit reports and event logs, the configuration management system, the effectiveness of the cyber security controls, and resolution of TCMs. The industry's annual operational costs for the periodic program reviews are provided in the Draft RA, Section 4.2.3, "Industry Annual Operations," subsection, "Periodic review and update procedures and supporting information." The estimated annual costs are $42,665 per FCF. The percentage of costs, identified in Table I-3 and described in Section I.6, associated with the substantial increase in overall protection are:

- 25 percent of the costs for Category I FCF licensees (three facilities);
- 25 percent of the costs for the Category III FCF licensee with classified information (one facility); and
- 100 percent of the costs for the Category III FCF licensees without classified information (three facilities).

The total annual costs are calculated as follows:

$$\frac{\$42{,}665}{\text{facility}} \times \left(3 \text{ facilities}\left(\frac{25\%}{100\%}\right) + 1 \text{ facility}\left(\frac{25\%}{100\%}\right) + 3 \text{ facilities}\left(\frac{100\%}{100\%}\right)\right) = \$170{,}660$$

These annual costs for industry are discounted at 3 percent per year over the average license period for FCFs, which is 25 years (drawn from the Draft RA, Section 3.2.3).

$$\$170{,}660 \times \frac{\left((1+0.03)^{25}-1\right)}{\left(0.03\times(1+0.03)^{25}\right)} = \$2{,}971{,}728$$

The total industry discounted cost over the estimated license period of 25 years is estimated to be $2,971,728.

V.3.2 Conducting configuration management – 10 CFR 73.53(f)

This provision would require that FCF licensees determine if facility changes adversely impact the cyber security program or create new VDAs. This provision would also require that FCF licensees to revise facility equipment and related procedures to resolve deficiencies. The industry's annual operational costs for the configuration management system are provided in the Draft RA, Section 4.2.3, "Industry Annual Operations," sub-section "Configuration management and threat awareness." The estimated annual costs are $28,607 per FCF. The percentage of costs, identified in Table I-3 and described in Section I.6, associated with the substantial increase in overall protection are:

- 25 percent of the costs for Category I FCF licensees (three facilities);
- 25 percent of the costs for the Category III FCF licensee with classified information (one facility); and
- 100 percent of the costs for the Category III FCF licensees without classified information (three facilities).

The total annual costs are calculated as follows:

$$\frac{\$28{,}607}{\text{facility}} \times \left(3 \text{ facilities}\left(\frac{25\%}{100\%}\right) + 1 \text{ facility}\left(\frac{25\%}{100\%}\right) + 3 \text{ facilities}\left(\frac{100\%}{100\%}\right)\right) = \$114{,}428$$

These annual costs for industry are discounted at 3 percent per year over the average license period for FCFs, which is 25 years (drawn from the Draft RA, Section 3.2.3).

$$\$114{,}428 \times \frac{((1+0.03)^{25}-1)}{(0.03\times(1+0.03)^{25})} = \$1{,}992{,}552$$

The total industry discounted cost over the estimated license period of 25 years is estimated to be $1,992,552.

V.3.3 Continuing training and maintenance – 10 CFR 73.53(d)

FCF licensees would incur annual operational costs to maintain their cyber security programs, which are estimated in the Draft RA, Section 4.2.3, "Industry Annual Operations Cost." This would include the costs to implement the cyber security refresher training for maintaining VDAs of $11,000 and refresher training for the Cyber Security Team of $16,000. The cost to maintain, modify, and test equipment to remain in compliance with the proposed regulations is estimated to be $25,000. The estimated annual costs to maintain the cyber security program are $52,000 per FCF. The percentage of costs, identified in Table I-3 and described in Section I.6, associated with the substantial increase in overall protection are:

- 25 percent of the costs for Category I FCF licensees (three facilities);
- 25 percent of the costs for the Category III FCF licensee with classified information (one facility); and
- 100 percent of the costs for the Category III FCF licensees without classified information (three facilities).

The total annual costs are calculated as follows:

$$\frac{\$52{,}000}{\text{facility}} \times \left(3 \text{ facilities}\left(\frac{25\%}{100\%}\right) + 1 \text{ facility}\left(\frac{25\%}{100\%}\right) + 3 \text{ facilities}\left(\frac{100\%}{100\%}\right)\right) = \$208{,}000$$

These annual costs for industry are discounted at 3 percent per year over the average license period for FCFs, which is 25 years (drawn from the Draft RA, Section 3.2.3).

$$\$208{,}000 \times \frac{((1+0.03)^{25}-1)}{(0.03\times(1+0.03)^{25})} = \$3{,}621{,}935$$

The total industry discounted cost over the estimated license period of 25 years is estimated to be $3,621,935.

V.4 Summary of estimated costs for the substantial increase in overall protection

The performance objectives in 10 CFR 73.53(b) are accomplished by implementing and operating the cyber security program. The detection, protection, and response capabilities are necessary to ensure cyber attacks do not result in a consequence of concern. Therefore, the costs associated with meeting the performance objectives represent the total costs for implementing and operating the cyber security program, as summarized in Table V-1.

Table V-1 Costs necessary for the substantial increase in overall protection

	Provision of the Cyber Security Program	Associated Cost (undiscounted)	Associated Cost at 3 percent over analysis period
Implementation Costs	Establishing the Cyber Security Team	$120,000	$120,000
	Creating a cyber security plan	$145,482	$145,482
	Completing the identification of VDAs	$594,000	$594,000
	Developing cyber security controls	$446,256	$446,256
	Implementing measures to ensure the protection of VDAs	$788,000	$788,000
Annual Costs	Completing periodic program reviews	$4,266,500	$2,971,728
	Conducting configuration management	$2,860,700	$1,992,552
	Continuing training and maintenance	$5,200,000	$3,621,935
Total cost to industry		$14,420,938	$10,679,953

V.5 Benefits

The NRC has identified quantitative and qualitative benefits that would result from implementation of the proposed rule. As discussed in this backfit analysis, quantitative

benefits are subject to uncertainty because the NRC staff cannot develop likelihood estimates for the events involving malicious cyber attacks, as they are not probabilistic. In addition, and for similar reasons, there is a significant range of magnitudes in consequences. Further, the staff identified two types of benefits, as presented below. The quantitative considerations include estimates of the averted costs, which are benefits consistent with guidance in NUREG-1409, Section 2.1.3(1)(b). The qualitative considerations include benefits from improvements in knowledge, regulatory efficiency, improved reliability, and public confidence. Both types of benefits support the conclusion that the provisions of the proposed rule associated with the safety consequences of concern are sufficient to cost justify the backfit analysis.

V.5.1 Quantitative Benefits (including significant uncertainties in probability and consequence)

As discussed in Section IV, preventing the active safety or latent safety consequences of concern by a cyber attack provides a substantial increase in overall protection of the public health and safety. This conclusion is based on the NRC staff's assessment of the threat environment and observed vulnerabilities in the cyber security programs at FCFs. This environment is discussed further in the Draft RA, Appendix B. The staff also assesses the quantitative benefits of the provisions of the proposed rule associated with the safety consequences of concern to range from $132,500 to $885,692,630 per incident, as noted in Table IV-1. To further analyze the significance of the range and magnitude of the potential benefits (in the form of averted costs) of these provisions in the proposed rule, and consistent with NUREG/BR-00058, Appendix A, "Qualitative Factors Assessment Tools," (ADAMS Accession No. ML15281A052), the staff performed a threshold analysis to estimate the number and magnitude of consequences of concern at which these provisions of the proposed rule would be cost beneficial. This analysis is illustrative because the likelihood of malicious cyber security events that result in consequences of concern is not known, as it is not probabilistic.

This analysis estimates the number of events, severity of impact, and related costs in relationship to the costs of implementing the proposed rule. The threshold analysis below provides a range of potential averted exposures which are considered benefits consistent with guidance in NUREG-1409, Section 2.1.3(1)(b). This range is based upon a number of assumptions to estimate the severity and frequency of events caused by malicious cyber attacks given the limited number of FCFs (i.e., 8) and their diversity in design and function.

Without the proposed rule, FCFs have the potential to experience cyber attacks that could result in consequences of concern during operations. The severity of the types of events identified by the threshold analysis are credible based on the types of accident scenarios in the licensee's ISAs. The potential for these types of events to occur during operations is plausible based on a number of factors including those discussed in the Draft RA, Appendix B. These factors include: (1) malicious cyber attacks have not been analyzed or protected against through the FCF licensees' ISAs (i.e., malicious cyber attacks could compromise existing safety systems resulting in intermediate or high consequence events previously determined through the ISA to be unlikely or highly unlikely, respectively); (2) the increase in the use of digital assets at FCFs; (3) the growing number of cyber attacks; (4) the increased potential of attacks from sophisticated adversaries; (5) the observed increase in cyber attacks on existing government, infrastructure, and power facilities around the world; and (6) the observed

variability in existing cyber security programs at FCFs.

For each type of event, the range of costs are calculated based on several assumptions. First, the low end of the range is calculated for a safety event that minimally meets the consequence of concern definition for only a single person. Second, the high range is calculated for a single safety event that results in the worst case health effects to the maximum affected population, based upon the applicable facility ISA.

In addition, the potential for multiple events over the lifespan of a facility's operations is supported by the NRC and industry observations of an increasing number of cyber security attacks on licensed facilities. Publically, FCF licensees have stated that averted cyber attacks have been observed to be occurring at a rate as high as 1000 attacks daily for some facilities. However, the majority of these attacks are considered low–impact (e.g. scanning for open communications ports by internet based "would be" attackers).

V.5.1.1 Methodology

The methodology to determine the benefits of the proposed rule requires consideration of the averted costs with significant uncertainty as to the number and potential magnitude of malicious events. As discussed in the Draft RA, Appendix B, there is substantial risk of a cyber attack resulting in a consequence of concern at FCFs.

The proposed rule requires FCF licensees to protect digital assets whose compromise could cause a consequence of concern with no credible alternate means of prevention (i.e., VDAs). For the purpose of this backfit analysis, the NRC staff estimates that a cyber attack on a VDA would cause a consequence of concern within the bounding range of events presented in Table V-8 below. An average number of operational years for the FCF licensees was estimated to be 25 years based on existing license terms as summarized in the Draft RA, Appendix A. Therefore the total number of licensed years of operations for 8 facilities is calculated to be:

$$8 \text{ facilities} \times \frac{25 \text{ average years of operations}}{\text{facility}} = 200 \text{ total years of operations}$$

This estimation provides a frequency for a single cyber security event to be:

$$\frac{1 \text{ event}}{(200 \text{ total years of operations})} = 5.0 \times 10^{-3} \text{ event/year}$$

Implementation of the proposed rule is estimated to reduce the frequency of an event having a consequence of concern with the defined measurable effects on occupational health to zero. This is because the proposed rule specifically states that FCF licensees must detect, protect against, and respond to a cyber attack capable of causing a consequence of concern. The proposed rule requirements of detection and protection of the VDAs through the application of appropriate cyber security controls, support the performance objective that the consequence of concern will not occur. In addition, maintenance of a response capability provides assurance that licensees will take action to stop cyber attacks before they can result in a consequence of concern. While licensees cannot and would not be required to prevent a cyber attack, the provisions of the proposed rule are designed to ensure that such an attack does not result in a

consequence of concern.

The proposed rule defines the health effects thresholds for safety consequences of concern, as an:

- exposure of 0.25 Sv (25 rem) or greater for any individual (i.e., worker or member of the public);
- intake of 30 mg or greater of uranium in soluble form for any individual outside the controlled area (i.e., member of public); or
- acute chemical exposure that could lead to irreversible or other serious, long-lasting health effects for any individual (i.e., worker or member of the public).

V.5.1.2 Exposure of 0.25 Sv (25 rem) or greater for any individual

The NRC staff reviewed potential FCF accident scenarios and found no off-site consequences that exceeded the 0.25 Sv (25 rem) threshold. For the purpose of this backfit analysis, an exposure of 0.25 Sv (25 rem) or greater is only credible for FCF employees on-site. The NRC further estimates that the number of individuals exposed due to a cyber security event would range from 1 to 10 (estimated maximum number of workers observed in a given area at a FCF licensee). An exposure of 0.25 Sv (25 rem) or greater can produce a range of health effects from increased risk to stochastic effects (e.g., cancer); serious, long-lasting injuries; or death of the exposed individual. The dollar value associated with this type of event can be presented in a range from $132,500 as a result of 0.25 Sv (25 rem) to a single individual (calculated using $5,300 (adjusted to 2016 dollars) per person-rem in NUREG-1530, Revision 1, "Reassessment of NRC's Dollar Per Person-Rem Conversion Factor Policy") to $9,000,000 (statistical life value in NUREG-1530, Revision 1 (ADAMS Accession No. ML15237A211)) per person as a result of a radiological exposure resulting in death.

In addition, this consequence of concern would result in on-site property damage. For the purpose of this backfit analysis, the refurbishment cost associated with cyber security events is estimated to be negligible. It would be unlikely for these types of events to damage equipment resulting in significant refurbishment costs. However, the cleanup and decontamination costs were estimated by adjusting the 1990 figures documented in Table C.6 of NUREG/BR-0184, "Regulatory Analysis Technical Evaluation Handbook" (ADAMS Accession No. ML050190193), to present day dollars. This produces a range of cleanup costs from $6,400 (minor radiological release confined to small areas in the facility) to $7,200,000 (criticality with 1/3 of the main building contaminated). Consistent with NUREG-1409, these averted onsite costs are considered negative costs in this backfit analysis.

Table V-2 Averted cost per minimum event – radiological exposure

Result of event	Injury	Death
Person(s) affected on-site	1	0
Person(s) affected off-site	0	0
Total person(s) affected	1	0
Cost per person	$132,500	$9,000,000
Subtotal cost	$132,500	$0
Clean-up and decontamination for on-site property	$6,400	
Total cost per event	$138,900	

Table V-3 Averted cost per maximum event – radiological exposure

Result of event	Injury	Death
Person(s) affected on-site	0	10
Person(s) affected off-site	0	0
Total person(s) affected	0	10
Cost per person	$132,500	$9,000,000
Subtotal cost	$0	$90,000,000
Clean-up and decontamination for on-site property	$7,200,000	
Total cost per event	$97,200,000	

V.5.1.3 Intake of 30 mg or greater of uranium in soluble form for any individual outside the controlled area

An intake of 30 mg or greater of uranium in a soluble form can produce serious and long-lasting health effects for the exposed individual. The dollar value associated with this event is presented as an averted cost of $397,500 (for a 30 mg intake[3]) per person. The worst case scenario (an intake of soluble uranium due to a 14-ton cylinder release) was considered based on the buoyant plume modeling results from the 2007 Response Technical Manual - 96 Supplement for Paducah Gaseous Diffusion Plant (ADAMS Accession No. ML073340013). The range of individuals exposed by this event is estimated to be from 1 to 142 people (based on the maximum public population in any population segment out to 0.6 mile of a FCF licensee[4]).

In addition, this consequence of concern would result in the spread of uranium both onsite and offsite. For the purpose of this backfit analysis, the refurbishment cost associated with these events is estimated to be negligible. It would be unlikely for these

[3] NUREG-1391, "Chemical Toxicity of Uranium Hexafluoride Compared to Acute Effects of Radiation," equates the chemical toxicity effects of an intake of 10 mg soluble uranium to the effects from a radiation exposure of 0.25 Sv (25 rem). Therefore, an intake of 30 mg of soluble uranium would roughly equate to 75 rem. NUREG-1530, Revision 1, provides a value of $5,100 person-rem. Adjusted to 2016 dollars provides a value of $5,300. Therefore, for the purpose of this backfit analysis, a 75 rem exposure having a statistical cost of $397,500 is roughly equal to the cost of an intake of 30 mg soluble uranium.

[4] 2010 Census data.

types of events to damage equipment resulting in significant refurbishment costs. However, the cleanup and decontamination costs were estimated by adjusting the 1990 figures documented in Table C.6 of NUREG/BR-0184 to present day dollars. This produces a range of cleanup costs from $6,400 (minor release confined to small areas in the facility) to $2,216,630 (major uranium hexafluoride (UF_6) release). Consistent with NUREG-1409, these averted onsite costs are considered negative costs in this backfit analysis.

Table V-4 Averted cost per minimum event – intake of 30 mg or greater of uranium in soluble form outside the controlled area

Result of event	Injury	Death
Person(s) affected on-site	N/A	N/A
Person(s) affected off-site	1	0
Total person(s) affected	1	0
Cost per person	$397,500	$9,000,000
Subtotal cost	$397,500	$0
Clean-up and decontamination for on-site property	$6,400	
Total cost per event	$403,900	

Table V-5 Averted cost per maximum event – intake of 30 mg or greater of uranium in soluble form outside the controlled area

Result of event	Injury	Death
Person(s) affected on-site	N/A	N/A
Person(s) affected off-site	142	0
Total person(s) affected	142	0
Cost per person	$397,500	$9,000,000
Subtotal cost	$56,445,000	$0
Clean-up and decontamination for on-site property	$2,216,630	
Total cost per event	$58,661,630	

V.5.1.4 Acute chemical exposure that could lead to irreversible or other serious, long-lasting health effects

An acute chemical exposure can produce a range of health effects to the exposed individual. NRC guidance does not provide a cost for this type of exposure. For the purpose of this backfit analysis, a moderate chemical exposure threshold is equivalent to Acute Exposure Guideline Levels-2 (AEGL-2) (irreversible or other serious, long-lasting adverse health effects or an impaired ability to escape – consistent with chemical exposure requirements in the ISA located in 10 CFR 70.61(b)(4)(ii) and (c)(4)(i)). The NRC staff calculated an estimate of the AEGL-2 cost equivalent by drawing on a review of U.S. Federal Aviation Administration (FAA) guidance on economic values for FAA investment and regulatory decisions (FAA, 2016). Section 2 of the FAA guidance provides the cost estimates for a moderate injury (i.e., an Abbreviated Injury Scale (AIS) level 2 (AIS-2) injury, which is defined as a major abrasion or laceration of skin, cerebral concussion (unconscious less than 15 minutes), finger or toe crush/amputation, or

closed pelvic fracture with or without dislocation). These injuries are comparable in scale to chemical exposures at the AEGL-2 level. For this threshold analysis, the loss of quality and quantity of life from an exposure at the AEGL-2 level is expressed as the same fraction (0.047) as is used for an AIS-2 injury of the value ($9,000,000) placed on an avoided fatality, which is equal to $423,000[5]. Therefore, the dollar value associated with an acute chemical exposure can be presented in a range from $423,000 to $9,000,000 (statistical life value in NUREG-1530, Revision 1) per person.

The number of individuals injured by the worst case scenario (an exposure of hydrogen fluoride (HF) due to a 14-ton cylinder release) is 10 people onsite (estimated maximum number of workers affected by the plume of HF in a given area at a FCF) and 206 people offsite[6] (based on the projected area affected in the buoyant plume modeling results from the 2007 Response Technical Manual - 96 Supplement for Paducah Gaseous Diffusion Plant). The number of individuals killed by the worst case scenario (an exposure of HF due to a 14-ton cylinder release) is estimated to be 2 people onsite (maximum number of workers fatally exposed to the plume of HF in a given area at a FCF) and 86 people offsite (based on the projected area affected in the buoyant plume modeling results from the 2007 Response Technical Manual - 96 Supplement for Paducah Gaseous Diffusion Plant).

In addition, this consequence of concern would result in on-site property damage from chemical contamination. For the purpose of this backfit analysis, the refurbishment cost associated with these events is estimated to be negligible. It would be unlikely for these types of events to damage equipment resulting in significant refurbishment costs. However, the cleanup and decontamination costs were estimated by adjusting the 1990 figures documented in Table C.6 of NUREG/BR-0184 to present day dollars. This produces a range of cleanup costs from $6,400 (minor release confined to small areas in the facility) to $2,216,630 (major UF_6 release). Consistent with NUREG-1409, these averted onsite costs are considered negative costs in this backfit analysis.

Table V-6 Averted cost per minimum event – acute chemical exposure

Result of event	Injury	Death
Person(s) affected on-site	1	0
Person(s) affected off-site	0	0
Total person(s) affected	1	0
Cost per person	$423,000	$9,000,000
Subtotal cost	$423,000	$0
Clean-up and decontamination for on-site property	$6,400	
Total cost per event	$429,400	

[5] "To establish a valuation for each AIS injury severity level, the level is related to the loss of quality and quantity of life resulting from an injury typical of that level. This loss is expressed as a fraction of the value placed on an avoided fatality." (FAA, 2016, citing Miller, 2010).
[6] 2010 Census data.

Table V-7 Averted cost per maximum event – acute chemical exposure

Result of event	Injury	Death
Person(s) affected on-site	10	2
Person(s) affected off-site	206	86
Total person(s) affected	216	88
Cost per person	$423,000	$9,000,000
Subtotal cost	$91,368,000	$792,000,000
Clean-up and decontamination for on-site property	$2,216,630	
Total cost per event	$883,368,000	

V.5.1.5 Analysis Conclusions

These analyses consider the costs for minimum and maximum impact scenarios for each safety consequence of concern. This results in a range of averted costs, bounded by a threshold exposure to a single person (i.e., lower bound) and the worst case scenario impacting a maximum population (i.e., upper bound), as summarized in Table V-8. These values are intended to provide bounded costs for a single event over the lifetime of all the FCFs.

Table V-8 Summary of averted cost per single event

Event	Cost description	Minimum averted cost	Maximum averted cost
Radiological exposure	Injury/death	$132,500	$90,000,000
	Clean-up/decon	$6,400	$7,200,000
	Total	$138,900	$97,200,000
Intake of 30 mg or greater of uranium in soluble form outside the controlled area	Injury/death	$397,500	$56,445,000
	Clean-up/decon	$6,400	$2,216,630
	Total	$403,900	$58,661,630
Acute chemical exposure	Injury/death	$423,000	$883,368,000
	Clean-up/decon	$6,400	$2,216,630
	Total[7]	$429,400	$885,584,630

Table V-9 provides several threshold values for the number of events and their corresponding severity at which the proposed rule's benefits exceed its costs. This table illustrates the event frequency and magnitude at which the rule becomes cost beneficial, in light of the significant uncertainty in risk and magnitude associated with a cyber attack that could cause a consequence of concern. The table considers four types of events: (1) multiple occurrences of the minimum consequence of concern (i.e., one person exceeding the threshold); (2) eight events with moderate impact (i.e., multiple individuals impacted in each event); (3) one event occurring across all FCFs with significant impacts (i.e., a large number of people impacted at once); and (4) one event that results in death

[7] The totals are the minimum and maximum costs for the direct harm due to a single event, and do not include costs to respond to the event, support NRC investigation, maintenance of safe facility conditions during response and recovery, and implementation of follow-on regulations to assure there is no recurrence.

Table V-9 Cost beneficial event frequency and magnitude

Safety consequence of concern	Events Over 25 Years	No. of People	Severity per event	Total averted cost[a] of described event necessary to exceed $14,420,938[8]
Radiological exposure of 0.25 Sv (25 rem) or greater for any individual	109	1	0.25 Sv (25 rem) total	$109\times1\times25\ \text{rem}\times\frac{(\$5300)}{\text{rem}}=\$14,442,500$
	8	Up to 10[c]	3.41 Sv (341 rem) total	$8\times341\ \text{rem}\times\frac{(\$5300)}{\text{rem}}=\$14,458,400$
	1	Up to 10[c]	27.21 Sv (2721 rem) total	$1\times2721\ \text{rem}\times\frac{(\$5300)}{\text{rem}}=\$14,421,300$
	1	2	Death	$1\times2\ \text{death}\times\left(\frac{\$9,000,000}{\text{death}}\right)=\$18,000,000$
	1	10	Death	$1\times10\ \text{death}\times\left(\frac{\$9,000,000}{\text{death}}\right)=\$90,000,000$
Intake of 30 mg or greater of uranium in soluble form for any individual outside the controlled area	37	1	30 mg intake of uranium	$37\times1\ (\text{30 mg exp.}^{b})\times\left(\frac{\$397,500}{\text{30 mg event}}\right)=\$14,707,500$
	8	5	30 mg intake of uranium	$8\times5\ (\text{30 mg exp.}^{b})\times\left(\frac{\$397,500}{\text{30 mg exp.}^{b}}\right)=\$15,900,000$
	1	37	30 mg intake of uranium	$1\times37\ (\text{30 mg exp.}^{b})\times\left(\frac{\$397,500}{\text{30 mg exp.}^{b}}\right)=\$14,707,500$
	0	0	Death	Not credible
	1	142	30 mg intake of uranium	$1\times142\ (\text{30 mg exp.}^{b})\times\left(\frac{\$397,500}{\text{30 mg exp.}^{b}}\right)=\$56,445,000$
Acute chemical exposure that could lead to irreversible or other serious, long-lasting health effects for any individual	35	1	AEGL-2 exposure	$35\times1\ (\text{AEGL-2 exp.}^{b})\times\left(\frac{\$423,000}{\text{AEGL-2 exp.}^{b}}\right)=\$14,805,000$
	8	5	AEGL-2 exposure	$8\times5\ (\text{AEGL-2 exp.}^{b})\times\left(\frac{\$423,000}{\text{AEGL-2 exp.}^{b}}\right)=\$16,920,000$
	1	35	AEGL-2 exposure	$1\times35\ (\text{AEGL-2 exp.}^{b})\times\left(\frac{\$423,000}{\text{AEGL-2 exp.}^{b}}\right)=\$14,805,000$
	1	2	Death	$1\times2\ \text{death}\times\left(\frac{\$9,000,000}{\text{death}}\right)=\$18,000,000$
	1	216	AEGL-2 exposure	$1\times216\ (\text{AEGL-2 exp.}^{b})\times\left(\frac{\$423,000}{\text{AEGL-2 exp.}^{b}}\right)=\$91,368,000$
	1	88	Death	$1\times88\ \text{death}\times\left(\frac{\$9,000,000}{\text{death}}\right)=\$792,000,000$

[a] Event does not consider additional cost of clean-up or decontamination

[b] The acronym "exp." stands for exposure per individual

[c] The radiological exposure could be distributed among up to 10 people (e.g., number considered for the bounding radiological exposure)

[8] The undiscounted costs necessary for the substantial increase in overall protection is used for the threshold analysis calculations in Table V-9. The estimated costs for events cannot be discounted because they could occur any time during the 25 years of operations.

and/or high exposure to large numbers of individuals (i.e., the bounding accident scenarios postulated in the ISA Summary for FCFs).

The types of events described in Table V-9 are representative of those that can occur at FCFs. These type of safety events involve consequences of concern which are based on the ISA requirements in 10 CFR Part 70, Subpart H. As discussed in the Draft RA, Appendix B, cyber attacks can impact safety systems directly (active consequence of concern) or indirectly by impacting the reliability of IROFS (latent consequence of concern). These types of events are considered credible safety events that could be caused by a cyber attack.

Although the NRC recognizes that the lower bound for events that result in a consequence of concern may occur more frequently, the NRC staff also notes that the goal of a cyber attacker would be to maximize the results of an attack.

V.5.2 Qualitative Benefits

The qualitative benefits of the proposed rule provisions associated with the safety consequences of concern relate to the reduced risk of malevolent use of SNM that the NRC staff believes would be achieved as a result of implementing these requirements. The staff is unable to quantify this reduction in risk due to the character of these benefits. In addition to the qualitative benefits associated specifically with the proposed rule provisions, the qualitative benefits of the overall rule include protection against consequences of concern from the DBTs and the protection of classified information, as further discussed in the Draft RA, Section 4.2.5, "Security and Safeguards Considerations." The new requirements will result in improved licensee cyber security programs, and thus the reliability of security and safeguards systems, that will reduce the overall risk from a cyber attack.

V.5.2.1 Improvements in Knowledge

The proposed requirement in 73.53(g), periodic review of the cyber security program, provides a means for a FCF licensee to gather valuable information that it can then use to maintain the effectiveness of its cyber security program. The analysis of FCF safety, security, and safeguards systems conducted as a part of a program review provides the FCF licensee with the qualitative benefit of an increased knowledge of the cyber security threat to facility digital assets. The requirement to maintain a qualified Cyber Security Team, analyze digital assets, document procedures, maintain a configuration management system, and conduct periodic reviews, contributes to a FCF licensee's knowledge of cyber security threats and vulnerabilities. As this knowledge increases, the anticipated risk of a successful cyber attack would be further reduced. Over time, a licensee's experience with implementing the cyber security program would lead to improvements in knowledge that further support effective cyber security program implementation.

V.5.2.2 Regulatory Efficiency

The proposed cyber security requirements would ensure that FCF activities (including the management and use of digital assets) are conducted safely and consistently. As described in Section I of this backfit analysis, FCF licensees have implemented a wide range of voluntary cyber security measures. Because there are no specific NRC

regulations governing cyber security requirements for FCF licensees, licensees may have implemented controls or programs that are more burdensome and/or less effective than the agency would require. This proposed rule would establish clear requirements for protection from cyber attacks capable of causing a safety consequence of concern. In addition, the regulatory guidance accompanying the rule would further inform approaches to an acceptable program. The proposed cyber security requirements therefore would provide the qualitative benefits of increased regulatory efficiency, as well as increased program effectiveness, and potentially reduced licensee costs.

V.5.2.3 Improved Reliability and Public Confidence

The proposed action would reduce the risk that a FCF licensee would suffer from lost production and revenue that could occur due to a cyber attack. The rule would require implementation of cyber security controls to meet performance objectives. In addition, the cyber security program would enhance public confidence in the licensees' ability to protect against cyber attacks as licensees would have implemented a comprehensive program with the objective of protecting against consequences of concern.

V.5.3 The Proposed Rule Is Cost Justified

In Section IV, the NRC staff concludes that the provisions of the proposed rule subject to a backfit analysis provide a substantial increase in the overall protection of the public health and safety. In this section (i.e., Section V), the staff concludes that these provisions are cost justified, as demonstrated by the staff's quantitative analysis. Although there is significant uncertainty in a successful cyber attack's frequency and impact on public health and safety, the proposed rule would protect against the specified safety consequences of concern. The averted costs associated with these safety consequences of concern exceed the estimated costs of implementing the proposed rule. Thus, the staff finds that the proposed rule is cost justified, and provides a substantial increase in the overall protection of public health and safety, and that therefore, backfitting is warranted.

VI. OTHER FACTORS FOR CONSIDERATION IN THE BACKFIT ANALYSIS

The NRC staff has considered the benefits and costs of the proposed rule, including the available information regarding credible threats, vulnerabilities, and safety consequences of concern. The staff has also considered information concerning the following nine factors identified in 10 CFR 70.76(b)(1)-(9). While this information is contained in the above analysis, it is called out in this section explicitly.

1. **Statement of the specific objectives that the proposed backfit is designed to achieve;**

   The proposed rule would amend 10 CFR Part 73 to implement cyber security requirements for certain FCF licensees. The objective of the new cyber security regulations in 10 CFR 73.53 would be to prevent a cyber attack from resulting in a safety consequence of concern. Section I.4 of this backfit analysis provides additional information on the specific objectives of this backfit.

2. **General description of the activity that would be required by the licensee or applicant in order to complete the backfit;**

   The proposed rule would require licensees to meet cyber security performance objectives. This involves creation of a team to implement the cyber security program. The team would identify the cyber security controls to be applied to VDAs. The controls provide protection of the VDAs. The program and controls would be documented in the cyber security plan. Licensees would provide ongoing configuration management augmented by periodic reviews to maintain the effectiveness of the program over time. Additional description of the activities required to complete the backfit are provided in Section I.4 of this backfit analysis.

3. **Potential change in the risk to the public from the accidental release of radioactive material and hazardous chemicals produced from licensed material;**

   The cyber security program reduces the risk of safety consequences of concern due to radiological and chemical exposures. The proposed rule provides a substantial increase in the overall protection of health and safety to reduce the risk of releases to the public as a result of a compromise of VDAs due to a cyber attack, that results in a safety consequence of concern. The protective measures, controls, and response capabilities established through the proposed rule reduce the likelihood of a release by protecting VDAs. Section IV of this backfit analysis describes the substantial increase in overall protection due to the provisions of the proposed rule associated with safety consequences of concern that reduce the risk of a release to the public.

4. **Potential impact on radiological exposure or exposure to hazardous chemicals produced from licensed material of facility employees;**

   The cyber security program would protect against the safety consequences of concern due to radiological and chemical exposures. The proposed rule provides for the protective measures, controls, and response capabilities to protect the health and safety of FCF employees and the public. Section IV of this backfit analysis describes the substantial increase in overall protection due to the proposed rule which reduces the potential for radiological or chemical exposures due to safety consequences of concern.

5. **Installation and continuing costs associated with the backfit, including the cost of facility downtime;**

Installation and Continuing Costs

The backfit analysis provides the NRC's estimate of affected licensees' implementation and annual operational costs for the proposed rule provisions associated with safety consequences of concern. Section V of this backfit analysis provides the costs, derived from the Draft RA, for each of these provisions of the proposed rule.

Potential Impact of Facility Downtime

The provisions of the proposed rule can be implemented without requiring facility downtime. The cyber security controls can be implemented for VDAs without interfering with facility operations because most of the controls are administrative in nature, limit access, or provide for additional monitoring (see the list of controls in Appendix B – F of the draft regulatory guide (ADAMS Accession No. ML16319A320)). The Cyber Security Team is required to conduct testing of cyber security controls in a test environment prior to implementation. If implementation of a control could result in facility downtime, licensees may implement TCMs that provide an equivalent level of protection for VDAs during operations until appropriate permanent controls are implemented.

6. **The potential safety impact of changes in plant or operational complexity, including the relationship to the proposed and existing regulatory requirements;**

The requirements of the proposed rule impose some increase in the complexity of the facility operations due to the added protective measures, controls, and response capabilities. This increase is expected to be offset by improvements in safety and security, especially the ability of the facility to protect against the safety consequences of concern.

In addition, the thresholds for the safety consequences of concern (proposed 10 CFR 73.53(c)(1)-(4)) are informed by existing regulatory requirements (i.e., 10 CFR Part 70). Utilizing existing regulatory requirements to inform the proposed rule reduces the potential impact of changes in plant or operational complexity. By using similar event thresholds, licensees can draw upon existing programs (e.g., security plan and ISA) to inform cyber security program management. The proposed rule would also allow FCF licensees to credit current safety and security measures to protect against cyber attacks, in lieu of providing new cyber security controls. The proposed 10 CFR 73.53 (d)(4) limits the scope of the rule to VDAs (i.e., those digital assets that have no alternate means to prevent a consequence of concern). As a result, the scope of affected safety and security systems is reduced.

7. **The estimated resource burden on the NRC associated with the proposed backfit and the availability of such resources;**

The NRC staff would experience some burden due to the proposed regulatory action.

Implementation Burden

Rulemaking

The NRC staff would create the proposed and final rule packages, associated guidance, and inspection procedures to support the rulemaking. This effort requires staff support for rulemaking activities over a multiyear period. To revise and update guidance documents (DG-5062) would require additional NRC resource expenditure. In addition, the NRC would incur additional contractor support costs for the implementation of the rule. The analysis assumes that the NRC's one-time implementation costs associated with the rule development and associated guidance development occurs in the years 2016-2018.

Create inspection procedures and training

The NRC staff plans to develop inspection procedures to reflect the new regulations. The staff estimates this would take 480 labor hours to complete. In addition, Region II personnel would need to be trained on the new inspection procedures. The staff estimates this training would take 40 labor hours for each FCF. Eight sites equals 320 hours total.

Review of cyber security plans and conduct two initial cyber security inspections

The NRC staff plans to review each FCF licensees' cyber security plan. This is estimated to take 100 hours of effort per plan. The initial inspection would be 20 labor hours per FCF and involve a review of the licensee's VDA identification activities. The second inspection, which would also be 20 labor hours per FCF, would involve review of the licensee's implementation of its full cyber security program.

Table VI-1 NRC implementation cost

NRC Implementation Cost	Labor hours	Mean/Best Estimate ($127.5/hour)
Rulemaking	8,520	($1,091,000)
Update guidance	1,420	($182,000)
Contractor support	N/A	($400,000)
Create inspection procedures and training	800	($102,000)
Review Cyber Security plans and initial inspection	1,120	($143,000)
Number of licensees	N/A	8
Total NRC Implementation Cost		($1,918,000)

NRC Operations Burden

The NRC would incur the cost to inspect FCF licensees to ensure compliance with the new proposed cyber security regulations. The NRC staff estimates these inspections would represent an incremental increase to the current inspection

schedule. In addition, the staff anticipates averaging one inspection per FCF licensee annually. The labor hours for an inspection would likely vary by licensee; however it is estimated, on average, to require 80 hours per inspection per FCF licensee.

The NRC would incur the cost to review license amendment requests involving cyber security plan changes. The NRC staff estimates that each FCF licensee would submit a license amendment request for the cyber security plan an average of once per year. This would, on average, entail a 40 hour review by the staff.

Table VI-2 NRC annual cost

NRC Annual Cost	Labor hours	Mean/Best estimate
Inspections	80	($10,240)
Review of program changes	40	($5,120)
Number of licensees	N/A	8
Total NRC Annual Cost		($122,880)

Based on a 25-year analysis period and the information in the two previous tables, the total cost to the NRC for the development and implementation of the proposed rule can be estimated at $4,990,000.

For additional details regarding the cost to the NRC, please see the Draft RA, Sections 4.2.2 and 4.2.4.

8. The potential impact of differences in facility type, design, or age on the relevancy and practicality of the backfit; and

See Section VI of this backfit analysis.

Potential Impact of Differences in Facility Type

The proposed rule takes into account the different facility types that would be affected by the provisions of the proposed rule associated with the safety consequences of concern. The facility type determines which consequences of concern (10 CFR 73.53(c)) need to be evaluated for that facility, thus the rule is specifically tailored to apply differently to different facilities, as appropriate. Each consequence of concern requires a different group of controls that must be applied to protect the VDAs. For example, all FCF licensees must evaluate if they have VDAs that could be compromised resulting in safety consequences of concern. If so, the FCF licensee must apply the applicable controls. In contrast, only the Category I FCF licensees need to consider the latent DBT consequence of concern and any applicable VDA controls. Because the consequences of concern and the level of controls applied for protection are dependent on the facility type, the provisions of the proposed rule provide a practical approach for the different types of affected facilities.

Potential Impact of Differences in Design

The potential impact of the provisions of the proposed rule associated with the safety

consequences of concern due to differences in design, is minimal because of the flexibility built into the proposed rule. The proposed rule requires licensees to conduct analyses to identify the VDAs independent of design. The consequences of concern in the proposed rule define performance thresholds that must not be exceeded during an event. This allows FCF licensees to evaluate their operations against these high-level standards to identify and protect the VDAs as the licensee considers appropriate, consistent with the requirements. The proposed rule would also allow the licensees to identify their own controls to protect against the consequences of concern. In addition, the proposed rule provides flexibility for FCF licensees to credit alternate means of preventing a cyber attack, in lieu of applying cyber security controls to VDAs. Because the proposed rule provides for common thresholds to identify the VDAs, creation of site specific controls, and the option to apply alternate means, imposition of the provisions of the proposed rule associated with the safety consequences of concern will have minimal impacts on facilities of different design. This is because the rule specifically considers the different types of facilities that will be affected, and is accordingly flexible and performance oriented.

Potential Impact of Differences in Age

The potential impact of differences in age to the backfit is also minimal because of the flexibility in the rule discussed above, and because the proposed rule applies to digital assets, which can be introduced to a FCF at any point during licensed operations.

9. Whether the backfit is interim or final and, if interim, the justification for imposing the backfit on an interim basis.

The backfit is final.

Backfitting should be required

The provisions of the proposed rule associated with safety consequences of concern would impose backfitting on FCF licensees' systems, structures, components, or procedures to implement a cyber security program. Consistent with 10 CFR 70.76(a)(3), as described in Section IV, the NRC staff has demonstrated that these provisions of the proposed rule provide a substantial increase in the overall protection of public health and safety through effective implementation of the cyber security program to prevent safety consequences of concern. As further described in Section V, the staff has demonstrated that the costs for the proposed rule provisions associated with the safety consequences of concern are cost justified. Finally, consistent with 10 CFR 70.76(b), in Section VI the staff has appropriately addressed the other factors for consideration that are relevant and material to the proposed backfit.

VII. OVERALL CONCLUSION

The proposed rule constitutes backfitting against protected entities licensed under 10 CFR Part 70, Subpart H. However, as discussed above, the NRC staff finds that the proposed rule should be implemented. The staff finds the proposed rule is necessary to ensure that cyber attacks do not result in a consequence of concern. The proposed rule would protect public health and safety and promote the common defense and security.

Specifically, as discussed in Section III, those provisions of the proposed rule associated with the DBTs and protection of the classified information consequences of concern are necessary to ensure that the common defense and security are adequately protected. As discussed in Section IV, those provisions of the proposed rule associated with the safety consequences of concern would provide a substantial increase in the overall protection of public health and safety. As discussed in Section V, these safety provisions are also cost justified. Therefore, the NRC staff finds that the proposed rule constitutes a permissible backfit on protected entities, and recommends that the Commission issue the proposed rule.

REFERENCES

DG-5062, "Cyber Security Programs for Nuclear Fuel Cycle Facilities," U.S. Nuclear Regulatory Commission, Washington, DC, (ADAMS Accession No. ML16319A320).

FAA, "Economic Values for FAA Investment and Regulatory Decisions, a Guide – Final Report," U.S. Federal Aviation Administration, Washington, DC, September 2016. https://www.faa.gov/regulations_policies/policy_guidance/benefit_cost/

Miller, T. and Spicer, R., "Final Report to the National Highway Traffic Safety Administration: Uncertainty Analysis of Quality Adjusted Life Years Lost." Pacific Institute for Research and Evaluation, February 5, 2010.

NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, Gaithersburg, MD, April 2013.

NRC, Draft *Federal Register* notice, "Cyber Security at Fuel Cycle Facilities" U.S. Nuclear Regulatory Commission, Washington, DC, 2017, (ADAMS Accession No. ML17018A220).

NRC, "Draft Regulatory Analysis for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR 73.53)," U.S. Nuclear Regulatory Commission, Washington, DC, 2017, (ADAMS Accession No. ML16320A452).

NRC, "Rulemaking for Cyber Security at Fuel Cycle Facilities Regulatory Basis Document," U.S. Nuclear Regulatory Commission, Washington, DC, March 2016, (ADAMS Accession No. ML15355A466).

NUREG/BR-00058, Predecisional Appendix A, "Qualitative Factors Assessment Tools," U.S. Nuclear Regulatory Commission, Washington, DC, February 2017, (ADAMS Accession No. ML17023A321).

NUREG/BR-0184, "Regulatory Analysis Technical Evaluation Handbook," U.S. Nuclear Regulatory Commission, Washington, DC, October 22, 2010, (ADAMS Accession No. ML050190193).

NUREG-1391, "Chemical Toxicity of Uranium Hexafluoride Compared to Acute Effects of Radiation," U.S. Nuclear Regulatory Commission, Washington, DC, February 1991, (ADAMS Accession No. ML072610444).

NUREG-1409, "Backfit Guidelines," U.S. Nuclear Regulatory Commission, Washington, DC, July 1990, (ADAMS Accession No. ML032230247).

NUREG-1530, Revision 1, "Reassessment of NRC's Dollar per Person-Rem Conversion Factor Policy," U.S. Nuclear Regulatory Commission, Washington, DC, August 2015, (ADAMS Accession No. ML15237A211).

Draft Regulatory Analysis for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR 73.53)

U.S. Nuclear Regulatory Commission

Office of Nuclear Material Safety and Safeguards

Division of Material Safety, State, Tribal, and Rulemaking Programs

2017

Table of Contents

List of Figures

List of Tables

Executive Summary

The U.S. Nuclear Regulatory Commission (NRC) is proposing a rule to establish cyber security requirements for certain nuclear fuel cycle facility (FCF) applicants and licensees in Part 73 of Title 10 of the *Code of Federal Regulations* (10 CFR), "Physical Protection of Plants and Materials." The NRC currently has no comprehensive regulatory framework addressing cyber security at FCFs. The proposed regulation, if approved, would require FCF applicants and licensees within the scope of the rule to establish, implement, and maintain a cyber security program designed to promote common defense and security and to provide reasonable assurance that the public health and safety remain adequately protected against the evolving risk of cyber attacks.

The proposed requirements, if adopted, 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, these applicants or licensees are: (1) subject to the requirements of 10 CFR 70.60, "Applicability;" or (2) subject to the requirements of 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."

The proposed rule distinguishes FCF licensees according to the category of the facility: (1) 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material," licensees authorized to possess or use a formula quantity of strategic special nuclear material (SSNM) as defined in 10 CFR 73.2, "Definitions" (Category I FCF licensees); (2) 10 CFR Part 70 licensees authorized to possess or use SNM of moderate strategic significance as defined in 10 CFR 73.2 (Category II FCF licensees); (3) 10 CFR Part 70 licensees authorized to possess or use SNM of low strategic significance as defined in 10 CFR 73.2 (Category III FCF licensees); and (4) 10 CFR Part 40 licensees authorized to perform uranium hexafluoride conversion or deconversion (conversion and deconversion facility licensees).

In accordance with 10 CFR 73.20, "General performance objective and requirements," Category I FCF licensees must maintain a physical protection system designed to protect against both the design basis threat (DBT) for radiological sabotage and the DBT for theft or diversion of formula quantities of SSNM. Both DBTs include a cyber attack as a method that may be exploited by adversaries. All FCF licensees are also subject to the Interim Compensatory Measure (ICM) Orders issued in 2002 and 2003. For the FCF licensees that were issued NRC licenses after 2003, the requirements of the orders were either incorporated as license conditions or imposed through the issuance of separate orders. Hereafter, the ICM Orders and similar requirements implemented through license conditions are collectively referred to as "ICM Orders." Although the primary focus of the ICM Orders was a physical attack, the orders also contained a requirement that licensees evaluate computer and communication networks for safety and security concerns related to "cyber terrorism." The relevant NRC guidance focused on the impact of a cyber attack on emergency response and offsite support. In general, licensees responded that: (1) the cyber element of the attack would

have a minimal impact on emergency response and offsite support; and (2) network security would be watched going forward.

The cyber security requirements in the DBTs and ICM Orders were imposed as a result of the growing cyber threat environment. However, neither the DBTs nor the ICM Orders provide a comprehensive regulatory framework for addressing cyber security at FCFs. The NRC has not inspected implementation of cyber security requirements at FCFs and no NRC enforcement actions have been taken against FCF licensees for any cyber security related issues.

During site visits at FCFs, the NRC staff has observed that many FCF licensees have implemented voluntary cyber security measures, primarily designed to protect FCF corporate networks from a cyber attack. The staff has determined that the voluntary cyber security measures taken by FCF licensees do not derive from a comprehensive analysis of cyber security vulnerabilities and, in certain cases, address only a limited number of cyber security threats. Because the licensees' actions are voluntary and are not included in their security plans or as license conditions, the NRC has no oversight, inspection, or enforcement authority to evaluate the appropriateness of those actions or ensure their effective implementation.

The U.S. Department of Homeland Security, Federal Bureau of Investigation, and National Security Agency provide the NRC with periodic updates regarding the evolving cyber threat and the vulnerabilities affecting the nation's critical infrastructure. These briefings typically focus on the potential consequences that this threat poses to hardened (i.e., non-internet facing and protected against compromise) computer systems and networks. The NRC uses this information to inform its understanding of the cyber threats confronting its licensees, including FCF licensees. During NRC staff site visits at FCFs, the staff observed potentially exploitable vulnerabilities in licensee computer systems, networks, and digital assets. Many of these systems, networks, and assets were not hardened, and therefore were not adequately protected against a cyber attack. These observations were discussed in the final regulatory basis, "Rulemaking for Cyber Security at Fuel Cycle Facilities" (Agencywide Documents Access and Management System (ADAMS) Accession No. ML15355A466).

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 safety or security consequence of concern defined in the proposed rule. The key changes to the regulations would require FCF licensees to:

- Establish and maintain a cyber security program to implement a graded, consequence-based approach for the protection of digital computer systems, communications systems, and networks.

- Identify digital assets associated with safety, security (both physical and information), and safeguards functions that if compromised by a cyber attack, would result in a consequence of concern.

- Protect vital digital assets[1] (VDAs) by selecting, applying, and maintaining appropriate cyber security controls.

- Apply and maintain defense-in-depth protective strategies to ensure the capability to detect and respond to a cyber attack.

- Establish and maintain a configuration management system to ensure the cyber security program requirements remain satisfied.

- Establish, maintain, and implement an NRC-approved cyber security plan that describes how the cyber security program performance objectives are met.

- Periodically review the cyber security program to determine if it continues to be effective.

These changes are designed to strengthen the FCF licensee's ability to defend against the compromise of a safety or security function performed by VDAs at its facility to ensure that a cyber attack would not result in one of the following consequences of concern:

- 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);

- Radiological sabotage;

- Theft or diversion of formula quantities of SSNM;

- Loss of nuclear material control and accounting for SSNM;

- Unauthorized removal of SNM of moderate strategic significance;

- Loss of nuclear material control and accounting for SNM of moderate strategic significance; or

- Loss or unauthorized disclosure of classified information.

[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.

Benefits and cost

This regulatory analysis measures the incremental costs of the proposed rule relative to a "baseline" that reflects anticipated behavior in the event the NRC does not undertake any regulatory action (Alternative 1, the "no action" alternative). The analysis quantifies benefits and costs associated with four affected attributes: (1) industry implementation, (2) industry operation, (3) NRC implementation, and (4) NRC operations. Because of the inherent difficulties in determining the monetary value of some of the benefits associated with the affected attributes, the analysis includes 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.

The key findings of the analysis are as follows:

- **Cost to the Industry.** The proposed rule would result in an estimated, undiscounted, average 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., the eight FCFs expected to be operational during the period of analysis) would incur an estimated, undiscounted implementation 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 estimated, undiscounted implementation cost to the NRC of approximately $1,900,000, followed by an estimated, undiscounted, average, annual operational cost of approximately $120,000 over the regulatory analysis period.

- **Benefits.** The proposed rule would enhance regulatory clarity by establishing specific regulatory requirements for implementing the cyber security performance objectives set forth in the ICM Orders and the DBTs. In addition, the proposed rule would increase regulatory efficiency and effectiveness by establishing regulatory guidance that can be used both by the industry for implementing the new cyber security requirements and by the NRC staff for review and inspection of cyber security programs at FCFs. The establishment of specific requirements and development of guidance would eliminate inconsistent approaches to cyber security across the fuel cycle industry and reduce burden upon FCF licensees by requiring them to only address cyber security for those digital assets that if compromised by a cyber attack, would result in a defined consequence of concern. The proposed rule would provide increased assurance that FCFs are protected from cyber attacks capable of causing a consequence of concern.

Decision Rationale

The NRC staff considered two alternatives: (1) no action; and (2) rulemaking to amend 10 CFR Part 73. The proposed rule would require FCF licensees to establish, implement, and maintain a cyber security program designed to 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. Through their cyber security programs, FCF licensees would be required 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 NRC has selected the second alternative, which would result in costs to the NRC and FCF licensees. The NRC staff has identified quantitative and qualitative benefits that would result from implementation of the proposed rule. As discussed further in Section V.5 of the 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. ML117018A221), the identified quantitative benefits are subject to significant uncertainty. Because events involving malicious cyber attacks are not probabilistic, the staff cannot develop accurate estimates of the frequency of such events. The staff has concluded that the proposed rule is cost-justified because the benefits associated with preventing a consequence of concern from a cyber attack at FCFs outweigh the estimated costs associated with implementing the proposed rule's requirements. The staff has identified potential vulnerabilities in existing digital assets at FCFs that, if exploited by a successful cyber attack, could result in a consequence of concern defined in the proposed rule. The proposed rule is necessary to ensure that a cyber attack does not result in a consequence of concern at a FCF that would adversely impact the public health and safety or the common defense and security.

Table ES-1 Combined Implementation and Annual Cost Summary by Entity over the 25-year analysis period

Entity	One-time implementation costs	Recurring and annual operating costs	Total combined implementation and annual cost 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**

Glossary of Terms and Acronyms

The following are abbreviations of terms used in this Regulatory Analysis.

ADAMS	Agencywide Documents Access and Management System
AEA	Atomic Energy Act of 1954, as amended
DBT	design basis threat
CFR	*Code of Federal Regulations*
CST	cyber security team
BLS	Bureau of Labor Statistics
FCF	fuel cycle facility
FTE	full-time equivalent
ICM	interim compensatory measures
ISA	Integrated Safety Analysis
IROFS	item relied on for safety
MC&A	material control and accounting
NRC	U.S. Nuclear Regulatory Commission
OMB	Office of Management and Budget
PCN	process control network
SCADA	Supervisory Controls and Data Acquisition
SNM	special nuclear material
SSNM	strategic special nuclear material
VDA	vital digital asset

1.0 Introduction

This document presents a regulatory analysis of the NRC's proposed rule to establish cyber security requirements for FCF licensees in 10 CFR Part 73. The proposed rule would require FCF licensees to establish a cyber security program and implement specific requirements for protecting VDAs from a cyber attack. Compromise of these VDAs as a result of a cyber attack could result in a consequence of concern.

The Atomic Energy Act of 1954, as amended, (AEA) provides the NRC with the general authority to conduct this rulemaking. The authority citations in 10 CFR Part 40 and Part 70 refer to AEA Section 161, "General Provisions," which authorizes the NRC to establish rules, regulations, or orders governing the possession and use of special nuclear material, source material, and byproduct material. Additionally, the authority citations in 10 CFR Part 40 and Part 70 refer to AEA Section 63, "Domestic Distribution of Source Material," and Section 53, "Domestic Distribution of Special Nuclear Material," respectively. These two sections of the AEA require that the NRC establish, by rule, minimum criteria for the issuance of specific or general licenses for the distribution of source material and special nuclear material, depending upon the degree of importance to the common defense and security or to the health and safety of the public with respect to: (1) the physical characteristics of the material to be distributed; (2) the quantities of material to be distributed; and (3) the intended use of the material to be distributed.

1.1 Background

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 evaluate computer and communications networks, and address vulnerabilities as necessary. However, the NRC did not provide guidance on how to implement the cyber security requirement in the ICM Orders. 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, "Purpose and scope." 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 designed to protect against both the DBT for radiological sabotage and the DBT for theft or diversion of formula quantities of SSNM. Both DBTs include a cyber attack as a method that may be exploited by adversaries. However, current NRC physical protection requirements do not set forth specific regulatory requirements to address cyber attacks at Category I FCFs.

Pursuant to 10 CFR 70.62, "Safety program and integrated safety analysis," those Part 70 FCF licensees within the scope of the rule are required to establish and maintain a safety program that demonstrates compliance with 10 CFR 70.61, "Performance requirements." One element of the safety program is to conduct and maintain an Integrated Safety Analysis (ISA). In meeting the requirements for an ISA, licensees identify hazards (e.g., chemical or radiological), potential accident sequences, and the consequences and likelihood of potential accident

sequences, as well as each item relied on for safety (IROFS) – also referred to as plant features and procedures – identified under 10 CFR 70.61. Licensees are required to implement IROFS to mitigate or prevent accident consequences that have the potential to exceed exposure thresholds, both radiological and chemical, for workers and the public at both high and intermediate levels, as defined by 10 CFR 70.61. The NRC's regulations do not require FCF licensees to consider malicious acts, such as cyber attacks, when conducting and maintaining their ISA.

The safety program established and maintained under 10 CFR 70.62 ensures that each IROFS is available and reliable to perform its intended function when needed and meets the performance requirements of 10 CFR 70.61. During site visits at a sample of FCFs, the NRC staff observed digital IROFS being used to perform certain safety functions that were susceptible to potential cyber attack vectors. If not adequately protected, these IROFS have the potential to be compromised by a cyber attack and may not be available or reliable to perform their intended safety function during an event (i.e., may result in a safety consequence of concern).

The cyber security requirements in 10 CFR 73.54, "Protection of digital computer and communication systems and networks," and associated guidance in Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," were developed for power reactor licensees and applicants. Nuclear power reactors 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, FCF licensees represent a broad spectrum of facility types, processes, and potential consequences of concern that could result from a cyber attack. Given the scope of the differences among FCFs, and taking into account the differences between FCFs and nuclear 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.

The FCF licensees also use digital assets to perform safeguards functions. Safeguards are generally: (1) measures taken to deter, prevent, or respond to the unauthorized possession or use of significant quantities of SNM through theft or diversion; and (2) measures taken to protect against radiological sabotage of nuclear facilities. These measures include material control and accounting (MC&A) programs, in accordance with 10 CFR Part 74, "Material Control and Accounting of Special Nuclear Material," to provide control and accounting measures to detect theft or diversion of SNM from authorized locations and processes within a facility. These measures also include physical protection programs, in accordance with 10 CFR Part 73, to protect nuclear facilities and material against sabotage, malicious acts, and theft or diversion that result in the removal of licensed material from a facility. MC&A requirements work together with a licensee's physical protection program to create an integrated and complementary safeguards approach to the protection of SNM that results in more robust protection against radiological sabotage or theft and diversion of licensed materials. Some FCF licensees integrate digital assets into their MC&A and physical protection programs, and rely upon them for the operation of those programs. During site visits, the NRC staff observed that some of these digital assets, including MC&A assets associated with IROFS, were susceptible to potential cyber attack vectors. Currently, there are no specific NRC requirements for the protection of these digital assets from cyber attacks. If not protected, these digital assets have the potential to be compromised by a cyber attack and may not be available or reliable to

perform their intended safety or safeguards function during an event (i.e., may result in a latent safety/safeguards consequence of concern).

Digital assets associated with physical security of classified information at FCFs are also subject to risk of a cyber attack. Certain FCF licensees (i.e., Category I and Category III enrichment licensees) are subject to the security requirements of 10 CFR Part 95, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data," and must maintain a facility security clearance because they process and store National Security Information and/or Restricted Data. The classified digital systems and networks that process and store this information are subject to U.S. Department of Energy cyber security requirements. The proposed rule would specifically exclude classified systems accredited by another Federal agency from the rule provisions. The NRC staff is continuing to explore the possibility that the rulemaking would also exclude certain unclassified digital systems accredited by other Federal agencies. However, the digital assets (e.g., cameras and door alarms) associated with the physical security of these classified systems and information fall within the regulatory purview of the NRC as the cognizant security agency for these facilities. Currently, there are no NRC cyber security requirements in place to protect these types of digital assets from cyber attacks. If not protected, these physical security digital assets have the potential to be compromised by a cyber attack and may not be available or reliable to perform their intended security function during an event (i.e., may result in a security consequence of concern).

Some FCF licensees are implementing voluntary cyber security measures (e.g., forming a cyber security team (CST), conducting cyber security awareness training, controlling portable media, and establishing an incident response capability) to address cyber security concerns. The voluntary cyber security measures implemented by industry do not reflect a comprehensive analysis of cyber security vulnerabilities and, in certain cases, only address a limited number of cyber security controls. In addition, the voluntary cyber security measures are not consistently based on a robust risk-management methodology (e.g., National Institute of Standards and Technology Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems, Revision 1"), and have been implemented in a manner that results in an ad hoc approach to the application of cyber security controls. The NRC staff has determined that, based on the developing threat of cyber security attacks and the potential for a consequence of concern, the voluntary cyber security measures lack a level of rigor commensurate with the developing cyber security risk.

1.2 Statement of the Problem and Objectives for Rulemaking

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 (see Appendix B). In order to sufficiently protect their VDAs, it is essential that FCF licensees understand and take measures to protect against cyber security threats and potential attack vectors.

The NRC's FCF cyber security working group, established in 2010, reviewed cyber security measures currently in place at FCFs to determine how they protect digital assets from cyber attacks. In conducting this review, the working group specifically looked at digital assets performing, supporting, or associated with critical functions that, if compromised, could impact public health and safety or common defense and security.

As discussed in the final regulatory basis, some general areas of concern identified by the working group during these assessments included:

- Some process control networks (PCNs), where digital assets that perform safety, security, or safeguards functions reside, were not protected consistent with cyber security controls generally applied to corporate networks.

- Some PCNs, where digital assets that perform safety, security, or safeguards functions reside, were not supported and maintained consistent with the corporate networks.

- There appeared to be an overreliance on physical security programs (e.g., access control) to protect connections to the PCNs.

- Periodic cyber security reviews were not consistently tied to system updates or the performance of maintenance.

- There appeared to be limited capabilities to detect cyber attacks.

- The voluntary cyber security measures taken by FCF licensees provided limited cyber security controls on portable media, mobile devices, and the use of wireless technologies.

- Network architecture documents did not appear to accurately illustrate system connections between digital assets and dependencies between digital assets.

- The voluntary cyber security measures taken by FCF licensees provided limited cyber security controls for offsite connections.

From its assessment of FCF licensees, the NRC working group identified digital assets that require additional protection. If the compromise of one of those digital assets were to go undetected and unresolved, a cyber attack could directly result in a consequence of concern.[2]

Compromise of digital assets could result in the failure of IROFS. If the compromise goes undetected and unresolved, the associated digital assets may not function properly, which could then result in IROFS not performing their intended safety function during an event. For example, if a digital gauge is designated as an IROFS which is used to monitor and limit the concentration of uranium in a process system, it could be compromised to allow build-up of SNM, without warning, and result in a criticality. The proposed rule would protect against the compromise of digital assets that impact certain IROFS (i.e., those relied upon to prevent a

[2] "Compromise" means that the digital asset loses confidentiality, integrity, or availability of data or function. The term "compromise" has a broader meaning than the term "failure." Failure means that the intended function is not performed. Compromise means that either the intended function is not performed or that an alternate, undesired function occurs. For example, failure of a wireless signal typically means that the signal is lost. Compromise of a wireless signal means that the signal is being used to perform unintended functions that may be of a malicious nature. Many safety and security analyses previously conducted by FCF licensees consider only failure mechanisms and do not consider the effects of malicious compromise.

nuclear criticality or chemical/radiological release resulting in significant exposures to workers or members of the public). The proposed rule designates this compromise as a latent consequence of concern because the compromise would not be revealed until the IROFS is needed to perform its safety function.

Digital assets associated with operational and process safety functions may be compromised by a malicious act, directly causing a safety consequence of concern. For example, compromise of a digital controller may cause the rupture of a container (e.g., through dropping, over-pressurization, over-heating, or over-filling) resulting in a chemical or radiological exposure. This type of compromise of a digital asset is designated as an active consequence of concern because the compromise of the digital asset directly causes the event.

In addition, digital assets used to perform certain security functions (e.g., deter, detect, assess, delay, respond, or communicate) may require protection from cyber attacks. A compromise would cause the digital asset to be unavailable to prevent, mitigate, or respond to theft or diversion of SNM, radiological sabotage, loss or unauthorized disclosure of classified material. This type of event could involve the theft of a significant quantity of SNM which could be used to create a radiological dispersion device (e.g., dirty bomb). For example, the compromise of a digital controller on a camera, surveillance system, or alarm system may prevent the ability to detect or respond to a physical attack. The compromise of a digital asset that impacts safeguards or security systems is designated as a latent consequence of concern. The compromise would only have an impact if it occurs in conjunction with some other action like a physical attack on the facility.

The proposed rule would provide additional assurance of a licensee's capability to protect its facility against cyber attacks that could cause a consequence of concern. In recognition of advancing digital technology, the proposed rule would establish a regulatory framework for cyber security at FCFs by requiring a cyber security program to protect digital assets that if compromised by a cyber attack, would result in a consequence of concern. As licensees implement digital upgrades for various processes at their facilities, the potential for consequences of concern from a cyber attack will increase unless sufficient protection is provided. The NRC staff expects the proposed rule to minimize the risk of a cyber attack resulting in a consequence of concern at FCFs, thereby increasing the overall safety and security for FCF licensees. The proposed rule is consistent with the Commission's direction in the SRM to SECY-14-0147 for the staff to implement cyber security requirements necessary to ensure that FCF licensees protect the health and safety of the public and promote common defense and security.

2.0 Identification of Alternative Approaches

The following discussion describes the two alternatives being considered in this regulatory analysis, with additional analysis presented in Section 3.

2.1 Alternative 1: No Action

Alternative 1, the "no action" alternative, would maintain the regulations as written. Under this option, the NRC would not modify 10 CFR Part 73.

Under the "no action" alternative, the ICM Orders and the 2007 revision to the DBT regulations would provide the only cyber security requirements for FCF licensees. However, the ICM Orders and the revision to the DBTs in 10 CFR 73.1 do not provide FCF licensees with sufficient regulatory requirements or guidance to enable them to develop and implement a cyber security program to address the evolving cyber security threat confronting FCF licensees. In the absence of specific NRC requirements, FCF licensees have implemented limited, ad hoc, voluntary cyber security measures. Licensee voluntary cyber security measures do not obviate the need for a regulatory framework for addressing cyber security threats to FCF licensees. In addition, the voluntary cyber security measures do not include a complete set of controls for digital assets, which leaves facilities susceptible to potential vulnerabilities. Finally, these voluntary cyber security measures are not enforceable unless licensees incorporate them into their licensing basis.

Cyber attacks have increased in number, become more sophisticated, resulted in physical consequences, and targeted digital assets similar to those used by FCF licensees. Appendix B to this document provides additional information on the vulnerability of FCF licensees to the cyber threat. For the reasons discussed above, the NRC staff has determined that FCF licensees must establish and implement a more robust cyber security program to protect against this threat.

The "no action" alternative would avoid the costs that the proposed rule provisions would impose. This alternative is equivalent to the status quo and serves as a baseline against which other alternatives can be measured.

2.2 Alternative 2: Amend 10 CFR Part 73

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 performance objectives, the licensee would:

a. Establish and maintain a CST to implement the cyber security program.

   The proposed 10 CFR 73.53(d)(1) would require all FCF licensees to establish a CST that is adequately structured, staffed, trained, qualified, and equipped to implement the cyber security program. This provision would ensure that the licensee has a team with sufficient knowledge and authority to implement and maintain a cyber security program to protect the facility against the applicable consequences of concern.

b. 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.

   The proposed 10 CFR 73.53(d)(2) would require that all FCF licensees establish and maintain cyber security controls. These controls would be specific to each of the applicable types of consequences of concern.

c. Identify digital assets that if compromised by a cyber attack, would result in one of the following consequences of concern, which are specific to the facility type: latent – DBT; latent – safeguards; active – safety; and latent – safety and security.

The proposed 10 CFR 73.53(d)(3) would require all FCF licensees to consider the digital assets utilized throughout the facility for NRC licensed activities and determine those whose compromise could result in a consequence of concern.

The proposed 10 CFR 73.53(d)(4) would require identification of VDAs. 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, as specified in 10 CFR 73.53(c). A FCF licensee may credit alternate means to prevent the consequence of concern associated with a digital asset identified per the proposed 10 CFR 73.53(d)(3). This provision to identify VDAs and credit alternate means would enable the FCF licensee to refine the scope of the cyber security program and provide assurance to the NRC that VDAs are identified.

d. Protect VDAs by establishing and maintaining the implementing procedures that document the measures taken to address the performance specifications associated with the applicable cyber security controls.

The proposed 10 CFR 73.53(d)(5)(i) would require licensees to identify the cyber security controls applicable to the type of consequence of concern associated with a VDA.

The proposed 10 CFR 73.53(d)(5)(ii) would require all FCF licensees to establish and maintain the implementing procedures that document the measures, associated with the applicable VDAs, taken to address the performance specifications of the cyber security controls.

The proposed 10 CFR 73.53(d)(6) would require all FCF licensees having VDAs to establish and document temporary compensatory measures in the event the measures otherwise taken to address cyber security controls become degraded. In the event a cyber security control cannot be applied or fails to perform as intended, the licensee would be required to implement temporary compensatory measures to meet the cyber security program performance objectives. The temporary compensatory measures would be interim actions (e.g., disabling the VDA or temporarily increasing surveillance) designed to prevent the consequence of concern, until appropriate measures that meet the performance criteria of the cyber security controls or an alternate means are in place and confirmed to be functioning as intended. This provision would require FCF licensees to track temporary compensatory measures to completion, in order to confirm that measures are taken to address the performance specifications of the applicable cyber security controls.

e. Establish, implement, and maintain a site-specific cyber security plan that describes how the cyber security program performance objectives are met, and provides for incident response to a cyber attack capable of causing a consequence of concern.

The proposed 10 CFR 73.53(e) would require all FCF licensees to establish, implement, and maintain a cyber security plan for their licensed activities. The cyber security plan would describe how the licensee satisfies the requirements of the proposed 10 CFR 73.53, manages the cyber security program, and provides for incident response to a cyber attack capable of causing a consequence of concern. The plan would provide a methodology for the identification and protection of VDAs, describe the management measures for the cyber security program, and include a documented approach for the FCF licensee to respond to a cyber attack capable of causing a consequence of concern.

f. Establish and maintain a configuration management system to ensure the cyber security program requirements remain satisfied.

The proposed 10 CFR 73.53(f) would require all FCF licensees to utilize a configuration management system to ensure that changes to the facility are evaluated prior to implementation and do not adversely impact the ability to meet the cyber security program requirements. Under the configuration management system, the FCF licensee would evaluate any previously unidentified digital assets, or modifications to existing digitals assets that are included in the cyber security program, prior to implementing the associated change to the facility. A facility's VDAs may change over time as the facility is modified, and as such, there is the continued potential for new vulnerabilities to be exploited and cause a consequence of concern. This provision would require FCF licensees to evaluate potential changes to processes or assets to ensure that the changes would not negatively affect existing cyber security controls or create new vulnerabilities.

g. Periodically review the effectiveness of the cyber security program.

The proposed 10 CFR 73.53(g) would require all FCF licensees to perform a periodic review of the cyber security program. Category I FCF licensees would perform the subject review as a part of the annual security program review in accordance with the requirements of 10 CFR 73.46(g)(6), which necessitates a conforming change to those requirements to include the cyber security program. All other FCF licensees would perform a review of the cyber security program at least every 36 months. This review would include an audit of the effectiveness of the cyber security program including, but not limited to, applicable cyber security implementing procedures, controls, alternate means, and defensive architecture. The findings, deficiencies, and recommendations from this review would be tracked, addressed in a timely manner, and documented in a report to the licensee's plant manager and corporate management. This provision would ensure that the FCF licensee periodically confirms that the cyber security program meets the required cyber security program performance objectives (i.e., detect, protect against, and respond to a cyber attack capable of causing a consequence of concern).

h. Notify the NRC Operations Center of certain cyber security events and internally track other cyber events.

The proposed 10 CFR 73.53(h) would require all 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 all FCF licensees, within 24 hours of discovery, to 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, Category I and II FCF licensees would be required to internally record, within 24 hours of discovery, if a cyber attack compromises VDAs associated with certain safeguards consequences of concern.

i. Maintain certain documentation as records.

The proposed 10 CFR 73.53(i) would require all 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 all FCF licensees to maintain and make available for inspection all records, reports, and documents pertaining to the cyber security program, until the NRC terminates the license or for at least 3 years after they are superseded.

Items a, b, and f – i, as described above, contain programmatic requirements that would be applicable to FCF licensees. Items c – e, as described above, contain proposed provisions that would require FCF licensees to identify and protect certain digital assets that if compromised by a cyber attack, would result in a consequence of concern specific to the facility type. The proposed rule is intended to provide FCF licensees the ability to detect, protect against, and respond to a cyber attack capable of causing specific consequences of concern.

2.3 Other Approaches Considered

In developing the proposed rule, the NRC considered a number of additional approaches to improving cyber security at FCFs, including issuing generic communications, developing new guidance documents, and revising existing inspection modules or enforcement guidance. Because these approaches would not fully address the regulatory issues described above, the NRC did not evaluate them as alternatives to the proposed action.

The NRC staff presented the option to issue orders imposing specific cyber security requirements on FCF licensees in SECY-14-0147. SECY-14-0147 included a draft security order that specified requirements for a CST, cyber security awareness training, incident response capabilities, portable media controls, baseline inventory of digital assets, isolation of specific assets, development of applicable cyber security configuration management controls, and the reporting of certain cyber security events. In the SRM for SECY-14-0147, the Commission rejected the use of orders and directed the staff to proceed directly with a high-priority rulemaking. Based on the Commission's direction, the staff has not considered the issuance of orders as an alternative. Accordingly, this regulatory analysis does not contain an evaluation of the benefits and costs of issuing orders.

3.0 Estimation and Evaluation of Benefits and Costs

This section describes the analysis that the NRC conducted to identify and evaluate the benefits and costs of the two regulatory alternatives. Section 3.1 describes how the benefits and costs were analyzed. Section 3.2 presents the assumptions made in the analysis. Section 3.3 identifies the entities expected to be affected by the proposed rule. Section 3.4 identifies the attributes expected to be affected by the proposed rule.

3.1 Analytical Methodology

This section describes the methodology used to analyze the consequences associated with the proposed rule. The methodology for a regulatory analysis is specified by various guidance documents. The two documents that govern the NRC's regulatory analysis process are NUREG/BR-0058, Revision 4, and NUREG/BR-0184. In addition, the methodology is in accordance with guidance from the Office of Management and Budget (OMB), Circular A-4, "Regulatory Analysis."

Based on OMB guidance, present-worth calculations are presented using both 3 percent and 7 percent real discount rates. The real discounted rates or present-worth calculation determines how much society would need to invest today to ensure that the designated dollar amount is available in a given year in the future. By using present-worth calculations, benefits and costs are valued equally regardless of time. The 3 percent rate approximates the real rate of return on long-term government debt which serves as a proxy for the real rate of return on savings. This rate is appropriate when the primary effect of the regulation is on private consumption. Alternatively, the 7 percent rate approximates the marginal pretax real rate of return on an average investment in the private sector, and is the appropriate discount rate whenever the main effect of a regulation is to displace or alter the use of capital in the private sector. Current trends in the marketplace reflect returns on investments well below the 3 percent and 7 percent discount rates, upon which OMB Circular No. A-4 is based. The NRC staff is providing a zero discount rate (e.g., undiscounted values) as a further sensitivity analysis. The staff is reporting the undiscounted costs as part of the sensitivity analysis based on current market trends and future predictions.

In this regulatory analysis, the NRC staff identifies all attributes related to the regulatory action and analyzes them either quantitatively or qualitatively. For the quantified regulatory analysis, the staff developed expected values for each benefit and cost. First for each alternative, the staff determined the benefits and costs, and then discounted the consequences in future years to the current year of the regulatory action. Finally, the staff summed the benefits and costs for each alternative and compared them.

This regulatory analysis measures the incremental costs of the proposed rule relative to a "baseline" that reflects anticipated behavior in the event the NRC does not undertake any regulatory action (Alternative 1, the "no action" alternative). As part of the regulatory baseline used in this analysis, the NRC staff assumes full licensee compliance with existing NRC regulations. This alternative is equivalent to the status quo and serves as a baseline to measure against the other alternatives. Section 4 of this analysis presents the estimated incremental benefits and costs of the proposed rule relative to this baseline.

After performing the quantitative regulatory analysis, the NRC staff addressed attributes that could only be evaluated qualitatively. The proposed rule includes changes that would affect attributes in a positive but not easily quantifiable manner. For example, security and safeguards considerations would be impacted through decreased risk of a security-related event, such as theft or diversion of radioactive material and subsequent use for unauthorized purposes. Quantification of the risk would require estimation of factors such as: (1) the frequency of attempted theft or diversion, (2) the frequency with which theft or diversion attempts are successful (i.e., pre-rule), and would be successful (i.e., post-rule), and (3) the impacts associated with successful theft or diversion attempts. These estimations would be difficult to quantify. Increasing the security of high-risk radioactive material decreases this risk and increases the common defense and security of the nation. Other qualitative values that are positively affected by the decreased risk of a security-related event include regulatory efficiency and improvements in knowledge.

The benefits include any desirable changes in the affected attributes. The costs include any undesirable changes in affected attributes.

3.1.1 Sign Conventions

The sign conventions used in this analysis are that all favorable consequences for the alternative are positive, and all adverse consequences for the alternative are negative. For example, additional costs above the regulatory baseline are shown as negative values and cost savings and averted costs are shown as positive values. Negative values are shown using parentheses (e.g., negative $500 is displayed as ($500)).

3.1.2 Data

The NRC staff used input from subject matter experts, information in NRC documents, stakeholder comments, knowledge gained from past rulemakings, and information gained during public meetings and from correspondence to collect data for this analysis.

3.2 Assumptions

Assumptions that were used are identified throughout this document. For reader convenience, major assumptions are listed below:

3.2.1 General assumptions

Discounted dollar values

The NRC calculates benefits and costs over the entire analysis period, discounted at a 3 percent and 7 percent discount rate and expressed in 2016 dollars. To provide a more complete discussion of potential costs, the NRC is also reporting the undiscounted costs as part of the sensitivity analysis.

Licensee labor rates

Licensee labor rates were obtained from Bureau of Labor Statistics National Wage Data available on the Bureau of Labor Statistics (BLS) web site. The NRC selected an appropriate mean hourly labor rate depending on the listed industry and the occupation (e.g., information security) and multiplying that labor rate by 2.4 to account for pension, insurance, and other legally-required benefits and then adjusting the resultant rate to 2016 dollars. Because exact licensee hourly rates can vary significantly, the NRC uses nationwide mean hourly rates. This analysis uses the following hourly rates:

Information Security Analyst ($44.83*2.4=$107.59).
Physical Security Manager ($28.69*2.4=$68.86).
Computer and Information System Manager ($67.69*2.4=$162.46)
Licensing Assistants ($25.19*2.4=$60.46)
Industry Engineer- Safety ($40.18*2.4=$96.43)

NRC labor rates

The NRC's labor rates are determined using the methodology in Abstract 5.2, "NRC Labor Rates," of NUREG/CR-4627, "Generic Cost Estimates, Abstracts from Generic Studies for Use in Preparing Regulatory Impact Analyses." This methodology considers only variable costs that are directly related to the proposed rule. Currently, the NRC hourly labor rate is $128. The estimation of costs for the proposed rule is based on professional NRC staff full-time equivalent (FTE). Based on actual data from the NRC's time and labor system, the number of hours in 1 year that directly relates to implementation of assigned duties is 1,420 (1,420 was derived by taking the annual number of hours (2,080) and accounting for leave, training, and completing administrative tasks). Therefore, an NRC professional staff FTE hourly rate is based on 1,420 hours.

3.2.2 Assumptions of anticipated licensee actions

Submission of the cyber security plan

The analysis was based on the assumption that only facilities currently in operation or under construction would submit a cyber security plan. A provision in the proposed rule permits current licensees who are not in possession of licensed material (i.e., not in operation) to delay submission of a cyber security plan until 6 months prior to possessing licensed material. There is uncertainty surrounding the economic factors that influence construction of FCFs. Therefore for purposes of this analysis, costs have not been included for the four FCF licensees shown in Table 3-1 as having an NRC license but that have either halted or not started construction.

Creation of the CST and cyber security plan

The analysis was based on the assumption that the FCF licensees would begin their efforts to comply with the cyber security rule by appointing a security senior manager to oversee the creation of the CST. The CST would consist of experts in cyber security, safety operations, facility security, and licensing. It is assumed that the CST members would already be qualified in their area of expertise and need minimal additional training, thereby reducing training costs. This team would be made up of mostly existing personnel (who may be augmented by contract or temporary personnel during implementation).

The analysis was also based on the assumption that the CST would create the cyber security plan. The cost would vary by licensee. Once the plan is in place, the CST would create the elements of their site's cyber security program. Estimates of the number of industry labor hours and related costs to develop the cyber security program are delineated in Section 4.2 of this analysis.

Analysis of digital assets and addressing cyber security controls

The analysis was based on the assumption that the identification of digital assets would entail minimal documentation for individual assets and would begin with a review of onsite documentation, including the ISA, Security Plan, MC&A Plan, and other existing facility documentation. This review would involve the use of a generic identification process to produce a list of digital assets that if compromised by a cyber attack, would result in a consequence of concern. The subject list, consisting of the identified digital assets and the associated consequence of concern, would be the only required documentation for this step of the process in establishing a cyber security program.

The analysis was also based on the assumption that the process to identify VDAs would take the list of digital assets and consider whether an alternate means of preventing the consequence of concern can be credited. Documentation of alternate means (as discussed in the draft regulatory guide, DG-5062, "Cyber Security Programs for Nuclear Fuel Cycle Facilities" (ADAMS Accession No. ML16319A320)) would consist of a short statement describing how the consequence of concern is prevented.

Furthermore, the analysis was based on the assumption that the licensees would credit existing alternate means when determining VDAs. Costs for any new alternate means are not considered in this cost benefit analysis, because the costs are assumed to be equal to or less than the costs presented in Tables 4-3 and 4-4 for addressing the cyber security controls for the VDAs.

Execution and annual operational cost

The analysis was based on the assumption that once the plan and program elements are in place, the licensee would be required to maintain its cyber security program and incur the associated annual operational cost.

Scope and implementation

The analysis was based on the assumption that the implementation and annual operational costs would vary by licensee depending on the level of existing cyber security protection and the presence or absence of VDAs. The number and severity of the consequences of concern may vary by licensee, which would drive the security controls necessary for VDAs. In addition, certain Category I FCF licensees already have a cyber security program that would need to be adjusted to comply with the new requirements. The labor effort to complete the various elements described above would vary by licensee. The specific labor estimates and other related costs for licensees are detailed in Section 4.2 of this analysis.

3.2.3 Time Horizon

The analysis assumes that the final rule would be effective in 2018. The analysis also assumes that it would take on average, 2 years for the licensees to implement the new requirements, thus the licensee implementation cost would be incurred in calendar years 2018 and 2019. For this regulatory analysis, the costs, including the implementation cost, are discounted to 2016 dollars when applicable.

The applicability period for the impacted FCFs is estimated to average 25 years. This estimate is based on the sum of the average remaining license term across these types of facilities. As a result, on average, the licenses for the impacted licensees expire in 2043. Given that the rule is expected to be issued in 2018, the average remaining life for currently licensed FCFs would be 25 years from final rule issuance so that any recurring costs would be discounted over that time. The specific details related to the FCFs remaining life by facility is in Appendix A of this document.

3.2.4 Cost/Benefit Inflators

To evaluate the benefits and costs consistently, the analysis inputs are put into base year dollars. This analysis utilizes the BLS Inflation Calculator developed by the U.S. Department of Labor, BLS Consumer Price Index calculator at http://www.bls.gov/data/inflation_calculator.htm.

3.3 Affected Entities

The affected entities listed in Table 3-1 are those that could be impacted by any of the alternatives. Information reflected in Table 3-1 was taken from NUREG-1350, Vol. 28, NRC Information Digest, 2016-2017 Edition. As noted in Appendix A, four proposed facilities that would be subject to the proposed rule (i.e., American Centrifuge Plant, GE-Hitachi, Eagle Rock Enrichment Facility, and International Isotopes Fluorine Products, Inc.) have received NRC licenses but have no projected construction or operation schedule. These licenses expire between 2037 and 2052. Costs for these FCF licensees are uncertain because the NRC is not able to determine if, or when, these licensees would possess licensed material, and therefore, be subject to the provisions of the proposed rule. As such, costs for these FCF licensees were not included in this analysis. However, if these licensees proceeded to construct and operate facilities consistent with their licenses, the costs would be consistent with the appropriate category of facility, as discussed in Sections 4.2 of this analysis. Future discounting would depend upon when such a facility was required to comply with the proposed rule.

Table 3-1 Impacted Entities			
Licensee/Facility	**Location**	**Status**	**Type**
American Centrifuge Plant*	Piketon, OH	License issued, construction halted	Gas Centrifuge Uranium Enrichment
AREVA, Inc	Richland, WA	Active	Uranium Fuel Fabrication
Babcock & Wilcox Nuclear Operations Group	Lynchburg, VA	Active	Uranium Fuel Fabrication
Eagle Rock Enrichment Facility*	Idaho Falls, ID	License issued, construction not started	Gas Centrifuge Uranium Enrichment
Global Laser Enrichment, LLC*	Wilmington, NC	License issued, construction not started	Laser Enrichment Facility
Global Nuclear Fuel – Americas, LLC	Wilmington, NC	Active	Uranium Fuel Fabrication
Honeywell International, Inc.	Metropolis, IL	Active	Uranium Hexafluoride Production (10 CFR Part 40 licensee)
International Isotopes Fluorine Products, Inc.*	Lea County, NM	License issued, construction not started	Uranium Hexafluoride Deconversion Facility (10 CFR Part 40 licensee)
Louisiana Energy Services, Urenco USA	Eunice, NM	Active	Gas Centrifuge Uranium Enrichment
Nuclear Fuel Services	Erwin, TN	Active	Uranium Fuel Fabrication
Shaw AREVA MOX Services, LLC	Aiken, SC	Under construction (operating license under review)	Mixed Oxide Fuel Fabrication Facility
Westinghouse Electric Company, LLC	Columbia, SC	Active	Uranium Fuel Fabrication

* For the purposes of this analysis, this facility is not included because the NRC is not able to determine if, or when, the associated licensee would possess licensed material and, therefore, be subject to the provisions of the proposed rule.

3.4 Identification of Affected Attributes

This section identifies the factors within the public and private sectors that the proposed rule is expected to affect, using the list of potential attributes in Chapter 5 of NUREG/BR-0184 and in Chapter 4 of NUREG/BR 0058. This evaluation considered each attribute listed in Chapter 5 of NUREG/BR-0184. The basis for selecting those attributes is presented below.

Affected attributes include the following:

- Industry Implementation – This attribute accounts for the projected net economic effect on the affected licensees of installing or implementing mandated changes. These costs include procedural and administrative activities, equipment, labor, and materials. The proposed action would require licensees to make facility modifications and to revise their cyber security plans as well as other implementation activities. Licensees would be required to submit cyber security plans for NRC review and approval.

- Industry Operation – This attribute measures the projected net economic effect of routine and recurring activities required by the proposed regulatory action on all affected licensees. The proposed action would require licensees to conduct additional cyber security activities beyond those currently required. For example, licensees would be required to periodically review the effectiveness of the cyber security program.

- NRC Implementation – This attribute measures the projected net economic effect on the NRC of implementing the proposed regulatory action. Under the proposed action, the NRC would develop the proposed and final rule packages. In addition, the NRC would develop the draft and final guidance documents.

- NRC Operations – This attribute measures the projected net economic effect on the NRC after the proposed regulatory action is implemented. Additional inspection, evaluation, and enforcement activities are examples of such costs. Under the proposed action, the NRC Operations Center would respond to calls from licensees upon discovery by the licensee of an imminent cyber security threat or activity.

- Safeguards and Security Considerations – The proposed actions are intended to establish requirements that would provide reasonable assurance that activities involving SNM are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

- Public Health (Accident) – This attribute accounts for expected changes in radiation exposure to the public caused by changes in accident frequencies or accident consequences associated with the proposed regulatory action. The proposed changes relative to the regulatory baseline (Alternative 1) would reduce the risk that public health would be affected by radiological releases resulting from radiological sabotage.

- Improvements in Knowledge – This attribute accounts for the potential value of new information. The proposed requirements in 73.53(g), periodic review of the cyber security program, would help the licensee gather additional valuable information that would be used in the implementation and continued review of the effectiveness of its cyber security program. Also, the proposed reporting requirements in 73.53(h) would provide the NRC with useful information about cyber threats at FCFs. Analysis of this information would

help identify threat concerns and vulnerabilities that the NRC could share with other licensees and Federal partners as appropriate.

- Occupational Health (Accident) – This attribute measures health effects, immediate and long-term, associated with site workers because of changes in accident frequency or accident consequences associated with the proposed changes. The proposed action would reduce the risk that occupational health would be affected by radiological releases resulting from radiological sabotage.

- On-site Property – This attribute accounts for the expected incremental monetary effects on onsite property, including decontamination, and refurbishment costs. The proposed action would reduce the risk that on-site property would be affected by radiological or chemical releases resulting from radiological sabotage.

- Regulatory Efficiency – The proposed action would result in enhanced regulatory efficiency through regulatory and compliance improvements.

- Other Considerations – The proposed action would reduce the risk that the licensee would suffer from lost production and potential revenue that would occur due to a cyber attack. In addition, the cyber security program, when implemented, is expected to enhance public confidence in the licensees' ability to counter the growing threat of a computer-based attack from an outside threat actor or malicious insider. Public confidence would be expected to increase with the knowledge that an effective program is protecting both intellectual and real property, as well as providing for the safety of workers and members of the public.

Attributes that are not affected include the following: off-site property, public health (routine), general public, occupational health (routine), environmental considerations, and other government and antitrust considerations.

4.0 Presentation of Results

This section summarizes the benefits and costs estimated for the regulatory options. To the extent that the affected attributes could be analyzed quantitatively, the net effect of each option has been calculated and is presented below. However, some values and impacts could only be evaluated on a qualitative basis.

4.1 Alternative 1: No Action

This regulatory analysis measures the incremental impacts of the proposed rule relative to a "baseline," which reflects anticipated behavior in the event that the proposed regulation is not imposed. The baseline used in this analysis assumes full licensee compliance with existing NRC requirements, including current regulations and relevant orders.[3]

[3] NUREG/BR-0058, "Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission," which is the NRC's staff guidance for regulatory analyses, states that, "in evaluating a new requirement...the

By definition, the "no action" alternative, the baseline for the principal analysis, does not result in any change in benefits or costs.

4.2 Alternative 2: Rulemaking to Amend 10 CFR Part 73

This section presents the results by attribute broken down by impacted entity.

4.2.1 Industry Implementation

Cyber Security Team (10 CFR 73.53(d)(1))

The licensee would need to establish a CST responsible for the execution of the cyber security program. The CST would establish and implement the cyber security plan. It is assumed that the licensee would incur an estimated average cost of $40,000 in creating the CST.

Cyber security plan (10 CFR 73.53(e))

In developing the cyber security plan, the CST would identify and analyze site-specific conditions that impact the implementation of the cyber security program. The analysis was based on the assumption that licensees would utilize the NRC cyber security plan template and cyber security controls provided in the draft regulatory guide.

The licensee would incur the cost to create the cyber security plan as well as the cost for its implementation. This includes the cost to conduct the analysis to identify digital assets, identify and apply the alternate means of control, determine the VDAs, and apply cyber security controls to the VDAs. In addition, the licensee would implement compensatory measures to address controls which cannot be implemented as originally intended. It is assumed that the licensee would incur an estimated 520 labor hours on average to accomplish these tasks.

Table 4-1 Creation of the Cyber Security Plan

Create the cyber security plan	Labor hours	Mean/Best cost estimate
Creation of the team	n/a	($40,000)
Hours to develop cyber security plan (Security Mgr.)	40	($6,498)
Hours to develop cyber security plan (cyber security experts)	200	($21,518)
Hours to develop cyber security plan (Facility expert)	80	($5,508)
Hours to develop cyber security plan (Safety operations expert)	80	($7,715)
Hours to develop cyber security plan (licensing/administrative)	120	($7,255)
Per FCF		($88,494)
Number of licensees		8
Total		($707,955)

staff should assume that all existing NRC requirements have been implemented."

Analysis of digital assets (10 CFR 73.53(d)(3 and 4))

The licensee would need to conduct an analysis to identify digital assets, consider alternate means of control, and determine the VDAs. A licensee analyzes digital assets used throughout the facility to determine their potential to be compromised by a cyber attack resulting in a consequence of concern. The analysis would distinguish between digital assets that can be protected by alternate means (e.g., a physical barrier), and VDAs which require application of the cyber security controls, identified in the cyber security plan, to prevent the consequence of concern.

Table 4-2 Analysis of Digital Assets

Analysis to identify digital assets, consider alternate means of control, and determine the VDAs	Labor hours	Mean/Best estimate
Labor hours (Security Mgr.)	120	($19,495)
Labor hours (cyber security experts)	640	($68,859)
Labor hours (Facility expert)	320	($22,034)
Labor hours (Safety operations expert)	320	($30,858)
Labor hours (licensing/administrative)	120	($7,255)
Per FCF		($148,500)
Number of licensees		8
Total		($1,188,004)

Cyber security controls and implementing procedures (10 CFR 73.53(d)(4 and 5))

For VDAs, a licensee would need to establish implementing procedures that document the measures taken to address the applicable cyber security controls. Additional procedures may be needed to address the methods for incident response and to detect cyber attacks capable of causing a consequence of concern. The number of digital assets protected by alternate means would vary by licensee. For the purpose of this analysis, FCF licensees are estimated to have an average of 12 VDAs per facility. The NRC estimates that a licensee would have adequate staffing to address and complete the documentation associated with the measures for the cyber security controls for two VDAs per week. Cost associated with hardware modifications are accounted for in Table 4-4.

Table 4-3 Address Cyber Security Controls and Implementing Procedures

Address cyber security controls and implementing procedures for application of cyber controls to VDAs	Labor hours	Mean/Best estimate
Labor hours (Security Mgr.)	80	($12,996)
Labor hours (cyber security experts)	480	($51,644)
Labor hours (Facility expert)	240	($16,525)
Labor hours (Safety operations expert)	240	($23,144)
Labor hours (licensing/administrative)	120	($7,255)
Per FCF		($111,564)
Number of licensees		8
Total		($892,516)

Other industry implementation costs

Staff training (10 CFR 73.53(d)(5))

Training of licensee staff in connection with implementation of a cyber security program is assumed to principally involve two key members of the CST ($8,000 per person, $16,000 total). This training is provided to members of the CST who need cyber security qualifications to implement the proposed rule. Other members of the CST that provide management oversight, security, or safety expertise would not require the same level of training in cyber security. This training of key individuals would ensure that the CST members have appropriate knowledge and skills to effectively implement the cyber security program.

Cyber security awareness training is also anticipated to be necessary for site employees responsible for identifying and protecting VDAs. These individuals would need training on the applicable controls, implementing procedures, and configuration management requirements associated with the VDAs. The licensee costs to create and deliver this training are estimated to be $6,000 per facility. The number of personnel responsible for VDAs would vary by licensee, however, the average total cost of training per FCF is estimated at $5,000. This would result in an overall per FCF training cost of $11,000.

System modifications (10 CFR 73.53(d)(5))

Each FCF licensee is estimated to have, on average, costs of $120,000 to make modifications to specific VDA hardware and software. The NRC estimates that FCFs will have an average of 12 VDAs. The range of costs for specific hardware and software modifications is estimated at $5,000 to $15,000 per VDA. The NRC assumes an average cost of $10,000 for each of the 12 VDAs resulting in an overall cost of $120,000 for specific VDA hardware and software modifications. The hardware and software modification costs include equipment purchases, one-time fees, and installation.

There is an additional estimated cost for network software associated with protecting multiple VDAs or sets of VDAs. For the purposes of this analysis, the NRC estimates the cost for this network software to be $50,000 per FCF licensee. This estimate includes the costs of testing, studies, and installation of the network software. The total costs for system modifications are estimated to be $170,000 per facility.

Table 4-4 Other Industry Implementation Cost

Other cyber security implementation cost	Mean/Best estimate per FCF	Total industry cost
CST Training	($16,000)	($128,000)
Awareness Training	($11,000)	($88,000)
System modifications	($170,000)	($1,360,000)
Total	($197,000)	($1,576,000)

Table 4-5 Total Industry Implementation Cost

Total licensee implementation cost	Mean/Best estimate per FCF	Total cost
Cyber security plan	($88,000)	($708,000)
Supporting technical information	($149,000)	($1,188,000)
Procedures	($112,000)	($893,000)
Training and system modifications	($197,000)	($1,576,000)
Total	($546,000)	($4,365,000)

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

4.2.2 NRC Implementation

Rulemaking

The NRC would develop the proposed and final rule packages and revise guidance and inspection procedures to accommodate the requirements that would be added or modified by the proposed rule. This effort would require six FTE (8,520 hours) over a 2 year period. To revise and update the guidance documents would take one FTE (1,420 hours). In addition, the NRC would incur $400,000 in additional contractor support costs to implement this regulatory action. The analysis assumes that the NRC's one-time implementation costs associated with rule and guidance document development are incurred in fiscal years 2017-2018.

The associated draft regulatory guide is expected to be published in parallel with the proposed rule.

Create inspection procedures and training

The NRC would develop inspection procedures to provide guidance to inspectors responsible for reviewing licensee cyber security program implementation and compliance with the new regulatory requirements. The NRC estimates this would take 480 labor hours to complete. In addition, Region II personnel would need to be trained on the new inspection procedures. The NRC estimates this training would take 40 labor hours for each facility. Therefore, inspector training for cyber security at the eight FCF licensees is estimated at 320 hours total.

Review of cyber security plans and conduct implementation inspections

The NRC would review and approve each licensee's cyber security plan. This effort is estimated to take 100 hours per FCF licensee. Additionally, the inspections pertaining to compliance verification with respect to the proposed rule would involve two inspections per FCF licensee at an estimated 20 labor hours for each inspection.

Table 4-6 NRC Implementation Cost

NRC implementation cost	Labor hours	Mean/Best estimate
Rulemaking	8,520	($1,091,000)
Update guidance	1420	($182,000)
Contractor support	N/A	($400,000)
Create inspection procedures and training	800	($102,000)
Review cyber security plans and initial inspection	1,120	($143,000)
Number of licensees	N/A	8
Total NRC Implementation Cost		($1,918,000)

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

4.2.3 Industry Annual Operations

Once the licensee's cyber security plan and program elements are in place, the licensee would be required to maintain the cyber security program and incur the associated cost.

Cyber security program annual operational cost

The licensee, after establishing its cyber security program, would incur annual operational costs to maintain the program. Those annual operational costs are associated with training personnel, conducting site-specific analysis, and updating and maintaining procedures as well as other supporting technical information.

Periodic review and update of procedures and supporting information

The licensee would incur the cost of conducting periodic reviews and updating supporting policies, implementing procedures, site-specific analysis, and other supporting technical information associated with the cyber security program. This would include maintaining the documentation on the master set of cyber security controls, identifying new digital assets, screening of the digital assets, and providing for temporary compensatory measures when needed. In addition, the licensee would need to audit the cyber security program at a frequency based on the facility type. The results of the periodic review of the cyber security program would be documented in a report to senior management. The total effort associated with this periodic review is estimated to be 440 labor hours per FCF.

Configuration management and threat awareness

The analysis was based on the assumption that 80 labor hours annually would be needed for the licensees to maintain their cyber security configuration management system. These labor hours are expected to include conduct of a cyber security impact analysis to evaluate potential vulnerabilities, weaknesses, and risks introduced by changes in the system, network, environment, or emerging threats. Stakeholder feedback during the public meeting on August 25, 2016 (ADAMS Accession No. ML16271A019), indicated that FCF licensees would likely utilize a private threat intelligence service to maintain threat awareness. The inclusion of a private threat intelligence service would add an estimated $20,000 in cost per FCF licensee.

Tracking and reporting

Each licensee would incur the cost to track and report events. Reporting of cyber events would follow current licensee processes. Tracking of cyber attacks is estimated to take a total of 80 hours of effort per year for the cyber security experts. The reporting and tracking of cyber-related events is estimated to take 40 labor hours annually for the cyber security manager and 40 labor hours annually for the licensing manager.

Refresher training

The analysis was based on the assumption that cyber security refresher training would be conducted on an annual basis by each FCF licensee. The refresher training for personnel with access to VDAs is estimated at 1 labor hour per person. The hourly rates discussed in Section 3.2.1 of this document, support an estimate of $110 per hour for these individuals. The number of personnel with access to VDAs would vary by licensee, however, assuming 100 people, the total cost of refresher training per FCF is estimated to be $11,000.

The refresher training for the CST would be an additional cost. Assuming an average cost of $4,000 per training session and estimating that 4 members of the CST will each receive 1 session per year, the annual cost assumed for the CST refresher training is estimated to be $16,000 per FCF licensee.

Equipment maintenance, modification, and testing

On average, the cost for each licensee is estimated to be $25,000 annually to maintain the hardware, software, and make modifications necessary to remain in compliance with the proposed rule.

Recordkeeping

On average, each licensee is estimated to need 20 labor hours annually to maintain its records and ensure they are marked and handled in accordance with the requirements applicable to the type of information the records contain (e.g., safeguards and classified).

Table 4-7 Industry Annual Operations

Industry annual operations	Labor hours	Mean/Best estimate
Periodic review and update of procedures and supporting information		
Labor hours (security manager)	40	($6,498)
Labor hours (cyber security experts)	240	($25,822)
Labor hours (facility expert)	80	($5,508)
Labor hours (licensing/administrative)	80	($4,836)
Total per FCF		($42,665)
Number of licensees		**8**
Total Industry cost for review and updating of procedures and supporting information		($341,322)
Configuration management and threat awareness	**Labor hours**	**Mean/Best estimate**
Labor hours (cyber security expert)	80	($8,607)
Private threat intelligence service		($20,000)
Total per FCF		($28,607)
Number of licensees		8
Total		($228,859)
Tracking and reporting	**Labor hours**	**Mean/Best estimate**
Labor hours (security manager)	40	($6,498)
Labor hours (cyber security experts)	80	($8,607)
Labor hours (licensing/administrative)	40	($2,418)
Total per FCF		($17,524)
Number of licensees		8
Total tracking and reporting		($140,191)
Training, recordkeeping, equipment maintenance and modifications	**Labor hours**	**Mean/Best estimate**
Refresher training	n/a	($11,000)
CST refresher training	n/a	($16,000)
Equipment maintenance and modification	n/a	($25,000)
Recordkeeping	20	($11,017)
Total per FCF		($63,017)
Number of licensees		8
Total		($504,136)

Table 4-8 Industry Annual Cost

Total industry annual cost	Cost
Review and update of procedures and supporting information	($341,000)
Configuration management system	($229,000)
Tracking and reporting	($140,000)
Training, recordkeeping, equipment maintenance, and modifications	($504,000)
Total	($1,214,000)

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

4.2.4 NRC Operations

The NRC would incur the cost to inspect FCFs to ensure compliance with the proposed rule. The NRC staff estimates that these inspections would be added as part of the NRC's existing inspection program for security, safeguards, and safety. In addition, the staff estimates an average of one inspection per FCF would be conducted on an annual basis over the 25 year period of the analysis. The labor hours associated with these cyber security inspections would vary by licensee, however, the staff estimates that it would take an average of 80 hours to complete each inspection, which includes time for inspection preparation and closeout.

The NRC would incur the cost to review license amendment requests involving cyber security plan changes. The NRC staff estimates that each FCF licensee would submit a license amendment request, on average, once per year. The staff estimates a review time of 40 hours for each amendment request.

Table 4-9 NRC Annual Cost

NRC annual cost	Labor hours	Mean/Best estimate
Inspections	80	($10,240)
Review of program changes	40	($5,120)
Number of licensees	N/A	8
Total NRC Annual Cost		($122,880)

4.2.5 Security and Safeguards Considerations

The NRC staff has observed that FCF licensees use digital assets to perform security and safeguards functions. If the compromise of one of those digital assets were to go undetected and unresolved, the digital asset could fail to perform the intended security or safeguards function when needed during an event. This type of compromise could, in turn, result in a latent DBT, safeguards, or security consequence of concern as defined in the proposed rule.

The proposed rule would prescribe requirements for a cyber security program to protect against potential security and safeguards consequences of concern resulting from a cyber attack. Although the averted costs associated with preventing a latent DBT or latent safeguards consequence of concern cannot be accurately quantified, a potential range of events can be considered. A cyber attack that results in either of these consequences of concern would have the potential for the theft or division of moderate or strategic SNM. These types of events could

range from diversion of SNM with no societal impacts, up to theft of strategic SNM for use in a radiological dispersion device (e.g., dirty bomb) that endangers public health and safety. Licensee costs associated with a response to diversion of SNM could potentially include those associated with facility shutdown and inspection, updating the MC&A program, and accounting for the SNM. Based on discussions with FCF licensees during site visits, these costs could potentially range into the millions of dollars. The potential societal impact of a radiological dispersion device could far exceed licensee costs. In "Survey of Costs Arising From Potential Radionuclide Scattering Events" (ADAMS Accession No. ML103620077), individuals from Sandia National Laboratories estimated the remediation costs alone from a moderate radiological dispersion resulting from such a device would be in the range of $10 - $300 million per square kilometer. The total economic impact from such an event was estimated at many billions of dollars in the publication entitled "Assessment of the Regional Economic Impacts of Catastrophic Events: CGE Analysis of Resource Loss and Behavioral Effects of an RDD Attack Scenario" (available at https://www.ncbi.nlm.nih.gov/pubmed/21232064).

Similarly, the averted costs associated with preventing a latent security consequence of concern cannot be accurately quantified. A cyber attack causing the loss or unauthorized disclosure of classified information or matter may result in an adversary gaining unauthorized access to information which, by definition, would cause damage to the national security. The costs resulting from the damage done to national security resulting from the loss or unauthorized disclosure of classified information cannot be quantified.

The proposed rule would reduce the risk of a cyber attack causing a security or safeguards consequence of concern. However, the NRC is unable to quantify the benefits associated with this reduction in risk. This is due to uncertainties in determining the: (1) frequency of cyber attacks resulting in security or safeguards consequences of concern; (2) frequency of attempts at theft or diversion of SNM; (3) frequency with which theft or diversion attempts are, and would be, successful; (4) frequency of attempts to gain unauthorized access to classified information or matter; (5) frequency with which attempts to gain unauthorized access to classified information are, and would be, successful; and (6) averted costs associated with prevented thefts or diversions of SNM and unauthorized access to classified information. However, the protective measures, controls, and capabilities established through the proposed rule reduce the potential likelihood and severity of a cyber attack compromising security and safeguards systems relied upon to protect classified information or matter and SNM. Section III, "Exceptions to Backfit Analysis" of the draft backfit analysis, provides additional discussion of the security and safeguards considerations of the proposed rule that the NRC staff believes are necessary to ensure adequate protection, consistent with 10 CFR 70.76(a)(4), of the health and safety of the public and are in accord with the common defense and security.

4.2.6 Public Health (Accident)[4]

The NRC staff has observed that FCF licensees use digital assets to perform safety functions. If the compromise of one of those digital assets by a cyber attack were to go undetected and unresolved, the digital asset could fail to perform the intended safety function when needed during an event. This type of compromise could, in turn, result in a safety consequence of

[4] For the purpose of this analysis, the NRC staff considers the accidents referenced by this attribute to be the results of a consequence of concern caused by a cyber attack.

concern such as a nuclear criticality or chemical/radiological release resulting in significant exposures to members of the public (i.e., a latent consequence). Furthermore, the staff has noted operational and process safety functions that, if compromised by a cyber attack, could directly cause a safety consequence of concern (i.e., active consequence).

The proposed rule requires the identification of digital assets and support systems that if compromised by a cyber attack, would result in specific consequences of concern, including the release of radioactive material and hazardous chemicals potentially impacting members of the public. The protection of those digital assets by cyber security controls is required by the proposed rule if an alternate means cannot be credited to prevent an active consequence of concern or maintain the function needed to prevent, mitigate, or respond to a latent consequence of concern.

The public's health may be impacted if a cyber attack results in a radiological exposure, intake of soluble uranium, or exposure due to an offsite chemical release that exceeds the threshold for a consequence of concern. To quantify this potential outcome for each affected facility, the analysis would need to estimate the change in the accident frequency and risk associated with the action and report this as avoided exposure, converting to dollars. However, the NRC is unable to accurately estimate the reduction in accident frequency (i.e., successful cyber attack frequency) per FCF facility, and thus this attribute is expressed qualitatively. The NRC projects that the protective measures, controls, and response capabilities established through the proposed rule reduce the potential likelihood and severity of a cyber attack causing a consequence of concern impacting public health and safety.

A threshold analysis presented in Section V.5.1, "Quantitative Benefits" of the draft backfit analysis provides a quantitative review of the potential averted costs to the public's health from a consequence of concern due to a cyber attack.

4.2.7 Improvements in Knowledge

The proposed requirements in 10 CFR 73.53(g), would require licensees to conduct a periodic review of their cyber security program. This review would help the licensee gather additional valuable information that it could then use to implement the program and review the program's effectiveness. Licensees would also gain knowledge of the cyber threats affecting their facilities that would enable them to avoid the potential disruptions, lost business opportunities, and cost of restoring their facilities following successful cyber attack. Also, the proposed reporting requirements in 10 CFR 73.53(h) would provide the NRC with useful information about cyber threats at FCFs. Analysis of this information would help identify threat actors and vulnerabilities that the NRC could share with other licensees and Federal partners as appropriate.

4.2.8 Occupational Health (Accident)[5]

The NRC staff has observed that FCF licensees use digital assets to perform safety functions. If the compromise of one of those digital assets by a cyber attack were to go undetected and unresolved, the digital asset could fail to perform the intended safety function when needed during an event. This type of compromise could, in turn, result in a safety consequence of

[5] Accidents are the result of a consequence of concern caused by a cyber attack.

concern such as a nuclear criticality or chemical/radiological release resulting in significant exposures to facility employees (i.e., latent consequence). Furthermore, the staff also noted operational and process safety functions that, if compromised by a cyber attack, could directly cause a safety consequence of concern (i.e., active consequence).

The proposed rule requires the identification of digital assets and support systems that if compromised by a cyber attack, would result in specific consequences of concern, including radiological exposure or exposure to hazardous chemicals causing either an active or latent safety consequence to facility employees. The protection of those digital assets by cyber security controls would be required by the proposed rule if an alternate means cannot be credited to prevent an active consequence of concern or maintain the function needed to prevent, mitigate, or respond to a latent consequence of concern.

The health of employees at FCFs may be impacted if a cyber attack results in a radiological exposure, intake of soluble uranium, or exposure due to a chemical release that exceeds the threshold for a consequence of concern. To quantify this potential outcome for each affected facility, the analysis would need to estimate the change in the accident frequency and risk associated with the action and report this as avoided exposure, converting to dollars. However, the NRC is unable to accurately estimate the reduction in accident frequency (i.e., successful cyber attack frequency) per FCF facility, and thus this attribute is expressed qualitatively. The NRC projects that the protective measures, controls, and response capabilities established through the proposed rule reduce the potential likelihood and severity of a cyber attack causing a consequence of concern impacting occupational health and safety.

A threshold analysis presented in Section V.5.1, "Quantitative Benefits" of the draft backfit analysis provides a quantitative review of the potential averted costs to the workers from a consequence of concern due to a cyber attack.

4.2.9 Regulatory Efficiency

An important benefit of the proposed rule would be an increase in regulatory efficiency, effectiveness, predictability, and stability. Industry stakeholders have informed the NRC staff in public meetings that they have expended time and resources in trying to understand and meet the generic cyber security provisions in the ICM Orders and the DBTs. As discussed above, the proposed rule would clarify regulatory expectations and focus licensee cyber security efforts on protecting only those digital assets that if compromised by a cyber attack, would result in a defined consequence of concern. The proposed rule would establish specific requirements that enhance regulatory clarity and consistency and promote the efficient implementation and inspection of licensee cyber security programs at FCFs. The associated guidance can be used by FCF licensees in understanding and implementing NRC requirements, thereby reducing the likelihood of non-compliance with the rule. The benefits derived from this increased regulatory clarity and efficiency are not easily quantifiable.

4.2.10 On-site Property Damage

One potential benefit of the proposed rule would be the expected monetary savings to all affected licensees from averted facility damage costs, including decontamination and refurbishment costs. Estimating the effect of the proposed action on onsite property involves three steps: (1) estimate the reduction in accident frequency; (2) estimate potential onsite

property damage; and (3) calculate the potential reduction in risk to onsite property. The NRC is unable to accurately estimate the reduction in accident frequency per FCF licensee and thus this attribute is expressed qualitatively. The NRC projects that there would be a reduction in the overall risk of facility damage. The proposed requirements would improve the cyber security program and thus increase reliability of safety systems which would reduce the overall risk of facility damage from a cyber attack.

A threshold analysis presented in Section V.5.1, "Quantitative Benefits" of the draft backfit analysis provides a quantitative review of the potential averted costs to on-site property damage from a consequence of concern due to a cyber attack.

4.2.11 Other Considerations

The cyber security program, when implemented, is expected to enhance public confidence in the licensees' ability to protect against the growing threat of a cyber attack. Public confidence would be expected to increase with the knowledge that an effective cyber security program is protecting the safety of workers and members of the public. This attribute is expressed qualitatively because the NRC is unable to accurately estimate the benefit of increased public confidence in the operation of fuel cycle facilities.

4.2.12 Totals

Quantitative Results: Total Present Value for the Cost

Table 4-10 summarizes the combined implementation and annual costs by entity, over the 25-year analysis period for Alternative 2.

Table 4-10 Combined Implementation and Annual Cost Summary by Entity over the 25-year Period of Analysis

Entity	One-time implementation costs	Recurring and annual operating costs	Total combined implementation and annual cost 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

4.3 Benefits and Costs

This section presents the benefits and costs from the proposed rule. To the extent that the affected attributes can be analyzed quantitatively, the net effect of each alternative is calculated and presented below. However, some benefits and costs could be evaluated on a qualitative basis only.

The NRC has identified quantitative and qualitative benefits that would result from implementation of the proposed rule. As discussed further in Section V.5 of the draft backfit

analysis, quantitative benefits are subject to uncertainty because the NRC staff cannot develop likelihood estimates for the events involving malicious cyber attacks, as they are not probabilistic. In addition, and for similar reasons, there is a significant range of magnitudes in the potential consequences of a cyber attack at a FCF. This range of magnitudes produces a corresponding range of direct benefits that would be expected to accrue and indirect benefits that would result from risks that could be avoided.

Table 4-11 summarizes the results of the benefits and costs analysis. The rulemaking alternative results in additional costs when compared to the no-action alternative. The quantitative impact of the rulemaking alternative is estimated to cost between approximately $18.6 million and $25.6 million (7 percent and 3 percent discount rate, respectively).

Table 4-11 Summary Table of Benefits and Costs

Net Monetary Savings (or Costs) - Total Present Value	Non-Monetary Benefits/Costs
Option 1: No Action $0	*Qualitative Benefits and Costs:* None
Option 2: Amend 10 CFR Part 73 **Industry:** ($18.6 million) using a 7 percent discount rate ($25.6 million) using a 3 percent discount rate **NRC:** ($3.4 million) using a 7 percent discount rate ($4.1 million) using a 3 percent discount rate	*Qualitative Benefits:* Safeguards and Security: Increased level of assurance that FCFs are safeguarded from cyber attacks that could result in the malevolent use of SNM. Public Health (Accident): Reduced risk that public health would be affected by chemical or radiological releases resulting from a cyber attack. Occupational Health (Accident): Reduced risk that occupational health would be affected by chemical or radiological releases resulting from a cyber attack. On-Site Property: Reduced risk that on-site property would be affected by radiological releases resulting from a cyber attack. Improvements in Knowledge: Periodic review of the cyber security program would help the licensee gather additional valuable information that it could then use to implement the program and review the program's effectiveness. Regulatory Efficiency: The cyber security requirements in the ICM Orders and the DBTs are generic and have resulted in licensees implementing a broad range of cyber security programs across the fuel cycle industry. Because the cyber security requirements in the ICM Orders and the DBTs are generic, a licensee could enact programs that are more burdensome than the agency intended or could spend unproductive time trying to understand the requirements. The proposed rule clarifies regulatory expectations and focuses cyber security efforts on providing protection from cyber attacks capable of causing consequences of concern. In addition, the proposed rule would increase regulatory efficiency and effectiveness by establishing regulatory guidance which can be used both by the industry for program implementation and the NRC for review and inspection. Other consideration: The cyber security program is expected to enhance public confidence in the licensees' ability to counter the growing threat of a computer-based attack from an outside threat actor or malicious insider. Public confidence would be expected to increase with the knowledge that an effective program is protecting both intellectual and real property, as well as providing for the safety of workers and members of the public. Improved Reliability and Public Confidence: The proposed action would reduce the risk that a licensee would suffer from lost production and revenue that could occur due to a cyber attack. In addition, the cyber security program, when implemented, would enhance public confidence in the licensees' ability to protect against a cyber attack. This confidence would increase because licensees would be required to develop and implement an effective program to protect against the safety consequences of concern.

The threshold analysis presented in Section V.5.1, "Quantitative Benefits" of the draft backfit analysis, provides a quantitative review of the potential averted costs to the attributes: Public Health (Accident), Occupational Health (Accident), and On-Site Property. The threshold analysis identifies a large range of averted costs. This is due to the complexity of quantifying the scope and likelihood of events due to malicious attacks. Traditionally, the failure of hardware has a quantifiable frequency due to observed failure rates, but such is not the case for a malicious cyber attack. Therefore, more accurately quantifiable averted costs cannot be developed for the proposed rule.

This analysis included consideration of the costs for minimum and maximum events for each safety consequence of concern (see Table 4-12 below). This results in a range of averted costs, bounded by a threshold exposure to a single person (i.e., lower bound) and the worst case costs to a maximum population (i.e., upper bound), summarized in Table V-8 of the draft backfit analysis. These values are intended to provide bounded costs for a single event over the lifetime of all the FCFs.

Table 4-12 Summary of Averted Cost per Single Event

Event	Cost description	Minimum averted cost	Maximum averted cost
Radiological exposure	Injury/death	$132,500	$90,000,000
	Clean-up/ decontaminate	$6,400	$7,200,000
	Total	$138,900	$97,200,000
Intake of 30 mg or greater of uranium in soluble form outside the controlled area	Injury/death	$397,500	$56,445,000
	Clean-up/ decontaminate	$6,400	$2,216,630
	Total	$403,900	$58,661,630
Acute chemical exposure	Injury/death	$423,000	$883,368,000
	Clean-up/ decontaminate	$6,400	$2,216,630
	Total[6]	$429,400	$885,584,630

5.0 Uncertainty Analysis

As this analysis is based, in part, on estimates of numerical values, it is useful to conduct a sensitivity analysis of those variables having the greatest amount of uncertainty. A Monte Carlo/Latin hypercube sensitivity analysis was completed with the assistance of @Risk, a software program specially designed for conducting this type of analysis. The Monte Carlo approach provides an answer to the question: "what distribution of net costs results from multiple draws of the probability distribution assigned to key variables?"

[6] The totals are the minimum and maximum costs for the direct harm due to a single event, and do not include costs to respond to the event, support NRC investigation, maintain safe facility conditions during response and recovery, and implement follow-on regulations to assure there is no recurrence.

5.1 Uncertainty Analysis Assumptions

A Monte Carlo analysis allows a range of possible inputs to be assigned to a distribution that is sampled in the simulation. Monte Carlo simulations involve introducing uncertainty into the analysis by replacing the point estimates of the variables used to estimate base case costs with probability distributions. The simulation repeatedly generates inputs to its mathematical algorithm that are selected randomly from a distribution of the possible inputs. After 10,000 simulations, the analysis provides a distribution of the results for variations in the values modeled.

A Monte Carlo analysis requires the identification of the variables that are uncertain; in this analysis, the uncertain variables are those that make up the implementation costs for the FCF licensees. The specific variables in this analysis include the labor hours needed to develop and implement the required elements of the cyber security program, including: development of the cyber security plan; the analysis of digital assets; identification and implementation of cyber security controls; training; and hardware or software modifications. Implementation costs would vary by licensee depending on the level of existing cyber security protection and the presence or absence of VDAs at a particular FCF.

A simplistic approach for taking the variables into account is the Triangular (also known as Three Point Estimate) technique. This technique uses three estimates to define an approximation of the proposed rule's cost. This technique works as follows: low, high, and best estimates for each variable are developed. The values for the estimates are based on NRC staff expertise and stakeholder feedback.

For this analysis, the uncertainties in licensee implementation costs are expressed in terms of upper- and lower-bounds for the effort (labor hours) to implement the various elements of the cyber security program. No attempt was made to apply an uncertainty analysis to the quantitative benefits of the proposed rule because the uncertainties in frequency and scope of the consequences of concern that would be averted by implementation of the proposed rule cannot be accurately estimated.

The upper- and lower-bound estimates, as well as the NRC staff's best estimate, of the labor hours needed for licensees to implement the various elements of the cyber security program are presented in Table 5-1. The staff used the labor rate assumptions from Section 3.2.1 of this document to calculate the labor hour costs for these estimates. Using these estimated costs, the staff generated a number of uncertainty distributions using a Monte Carlo simulation with the @Risk software. This simulation provides a statistical summation that can be used to characterize the overall uncertainty of the analysis. The results of the Monte Carlo simulations can then be compared with the results presented in Table 4.11, "Summary Table of Benefits and Costs" to inform how the uncertainty in the costs compares with the range of benefits.

Table 5-1 Summarizes the variable assumptions in the analysis by licensee

Data Element	Low estimate	Best estimate	High estimate
Hours to develop cyber security plan (Security Mgr.)	20	40	80
Hours to develop cyber security plan (cyber security experts)	100	200	280
Hours to develop cyber security plan (Facility expert)	40	80	120
Hours to develop cyber security plan (Safety operations expert)	40	80	120
Hours to develop cyber security plan (licensing/administrative)	100	120	180
Number of licensees	8	8	8
Analysis to identify digital assets, consider alternate means of control, determine the VDAs	Low estimate	Best estimate	High estimate
Labor hours (Security Mgr.)	80	120	160
Labor hours (cyber security expert)	500	640	780
Labor hours (Facility expert)	280	320	400
Labor hours (Safety operations expert)	280	320	400
Labor hours (licensing/administrative)	80	120	160
Number of licensees	8	8	8
Address cyber security controls and implementing procedures for application of cyber controls to VDAs	Low estimate	Best estimate	High estimate
Labor hours (Security Mgr.)	60	80	120
Labor hours (cyber security expert)	300	480	540
Labor hours (Facility expert)	200	240	300
Labor hours (Safety operations expert)	200	240	300
Labor hours (licensing/administrative)	100	120	160
Number of licensees	8	8	8
Training and Software/Hardware Implementation cost	Low estimate	Best estimate	High estimate
Training	($25,000)	($27,000)	($40,000)
System modifications	($150,000)	($170,000)	($750,000)
Number of licensees	8	8	8
Total	($1,400,000)	($1,576,000)	($6,320,000)

5.2 Uncertainty Analysis Results

Figures 5-1 through 5-4 display the histograms derived using the Monte Carlo simulations based on the range of costs estimated in Table 5-1. For each histogram, ten thousand simulations were run. Each graph provides the most likely cost, the mean cost, and the standard deviation based on the range of values provided in Table 5-1.

Figure 5-1 Cyber Security Plan

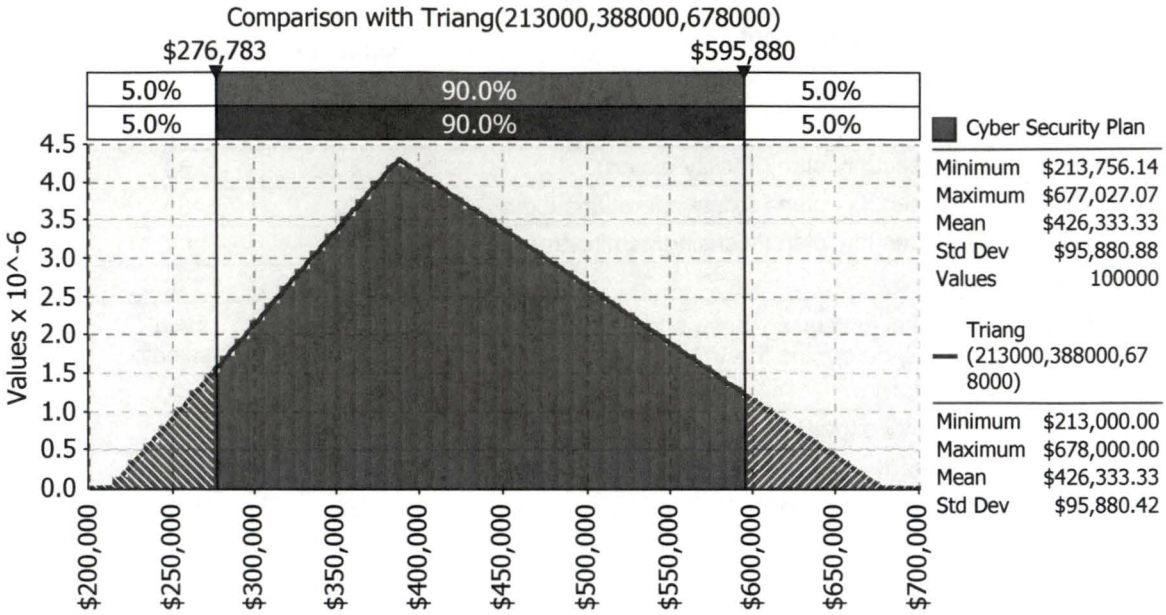


Figure 5-2 Analysis of Digital Assets

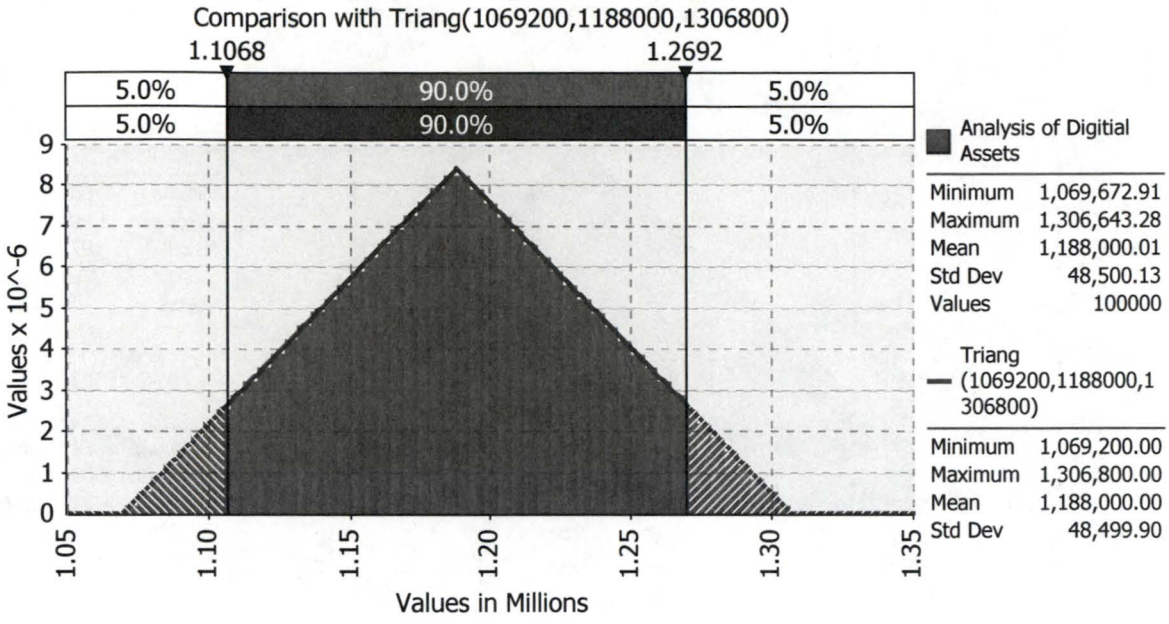


Figure 5-3 Cyber Security Controls

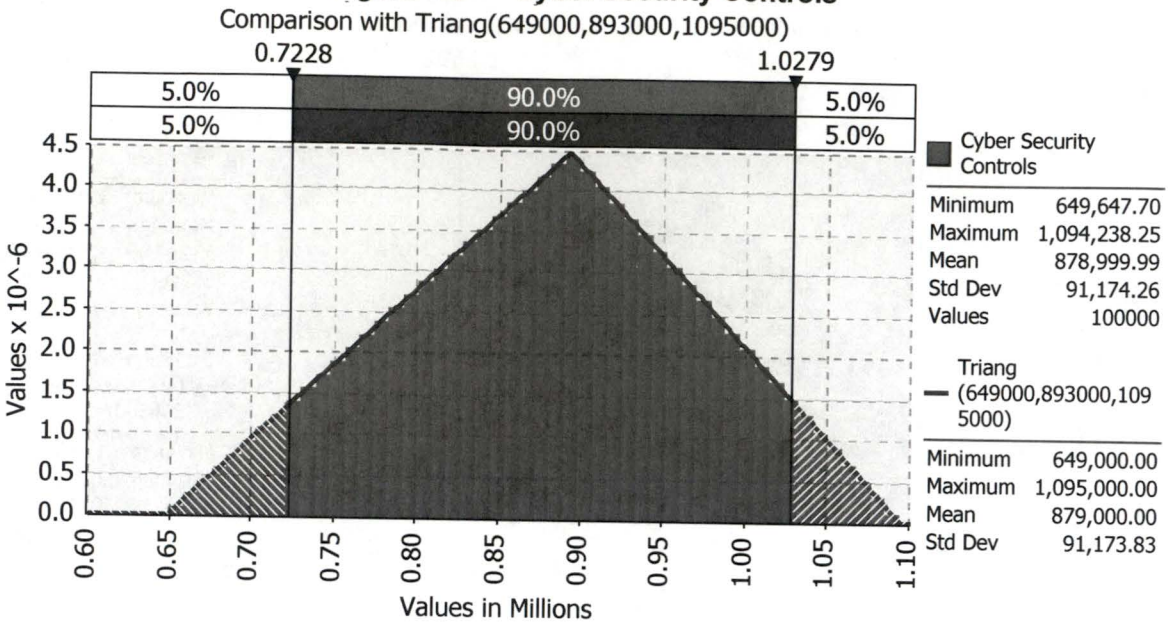
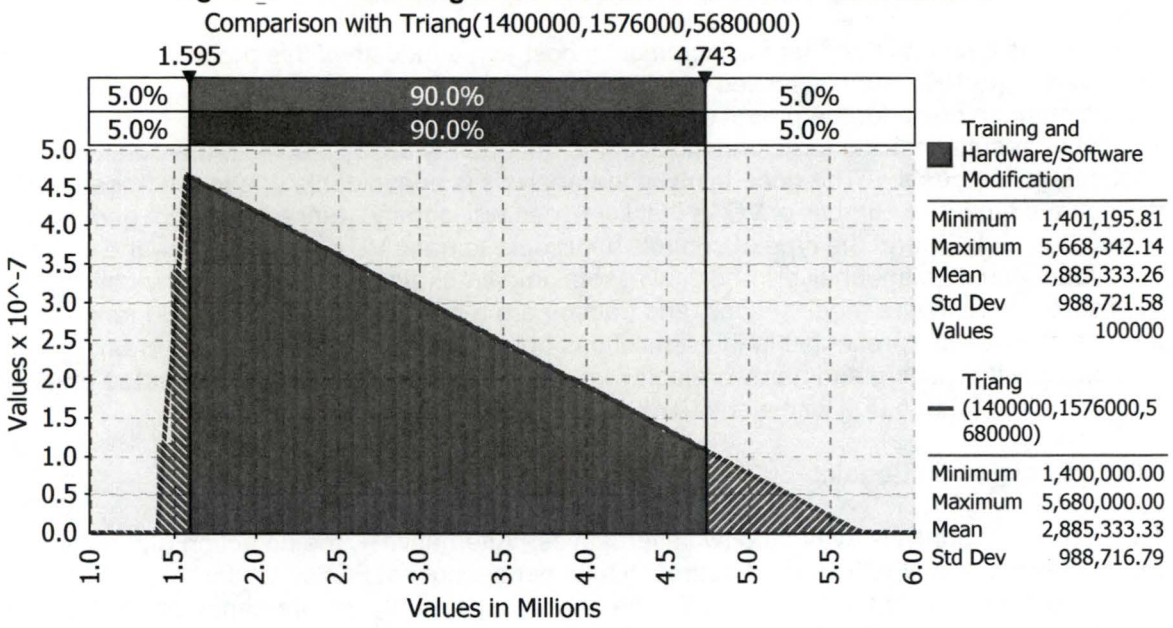


Figure 5-4 Training and Hardware or Software Modification



5.3 Summary of the Uncertainty Analysis

The analysis confirms that there is incremental cost to the industry if this proposed rule is approved. The NRC staff assessed which variables have the largest impact on total industry implementation costs for the proposed rule. As shown in Figures 5-1 through 5-4, the simulation results indicate large variations in the uncertainty associated with the potential implementation costs. The uncertainty in the analysis is unavoidable due to the absence of data on the type and number of VDAs that licensees will identify. Since the actual number of VDAs at each FCF and the type of controls applicable to each VDA are unknown, the costs for the cyber security plan, analysis of digital assets, implementation of cyber security controls, hardware and software modifications, and training are a best estimate with a large range of uncertainties. This is reflected in the simulations above. The largest uncertainty was associated with training and hardware/software modifications which had an estimated mean of approximately $2,885,000 with a standard deviation of $989,000.

6.0 Decision Rationale

This regulatory analysis evaluated two alternatives. Alternative 1, the no action alternative, would maintain the NRC's current approach to cyber security at FCFs. Under this option, the NRC would not modify 10 CFR Part 73. The only cyber security requirements for FCF licensees would be those in the ICM Orders and, for Category I FCFs, the requirement to protect against a cyber attack as part of the DBTs set forth in 10 CFR 73.1. Alternative 1 would avoid the costs that the proposed rule would impose on FCF licensees and the NRC. However, the NRC staff has determined that the ICM Orders and the DBTs do not provide licensees with sufficient regulatory requirements or guidance to enable them to develop and implement a cyber security program to address the evolving cyber security threat confronting FCFs.

Alternative 2 would amend the current regulations in 10 CFR Part 73, and make conforming changes to the regulations in 10 CFR Parts 40 and 70, to establish cyber security requirements for FCF licensees. The proposed regulation, if approved, would require FCF licensees within the scope of the rule to establish, implement, and maintain a cyber security program designed to promote common defense and security and to provide reasonable assurance that the public health and safety remain adequately protected against the evolving risk of cyber attacks. The FCF licensees, through their respective cyber security programs, would be required 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 principal qualitative benefit of the regulatory action would be the reduced risk of a cyber attack causing a consequence of concern at a FCF that would adversely impact the public health and safety or the common defense and security.

The proposed rule would provide a methodology for FCF licensees to identify digital assets having specific consequences of concern to public health and safety and the common defense and security. Furthermore, the proposed rule methodology would narrow the application of cyber security controls to only VDAs (i.e., those that have no alternate means to prevent the consequence of concern). The NRC staff concludes that the proposed rule would establish a predictable regulatory framework to address cyber security threats for FCFs. Additionally, the proposed rule would enable the NRC to develop an effective inspection program, reduce regulatory uncertainty, and address enforceability issues.

The NRC staff has concluded that the proposed rule is cost-justified because the benefits associated with preventing a consequence of concern at FCFs outweigh the estimated costs associated with implementing the proposed rule's requirements. Given the growing and evolving cyber security threat confronting FCF licensees, the proposed rule is necessary to ensure that a cyber attack does not result in a consequence of concern at a FCF that would adversely impact the public health and safety or the common defense and security. As discussed more fully in the draft backfit analysis, those provisions of the proposed rule associated with the protection of classified information and the DBT consequences of concern are necessary to ensure that FCFs remain adequately protected against a cyber attack. Those provisions of the proposed rule associated with safety consequences of concern provide a substantial increase in the overall protection of public health and safety that is cost justified.

7.0 Implementation

Table 7-1 presents the implementation schedule for the proposed rule.

Table 7-1 Implementation Schedule

Milestone	Timeframe
Licensee submits the cyber security plan, through an application for amendment of its license, to the NRC for review	Within 180 days of publication of the final rule or 6 months before the anticipated date for possessing licensed material
The NRC reviews and approves the license amendment request and cyber security plan	Typically within 150 days of submission
Licensee conducts analyses to identify and document each digital asset associated with a consequence of concern and determines: (1) VDAs and (2) digital assets with an acceptable alternate means	Within 6 months of NRC approval of the cyber security plan.
Full implementation of the NRC approved cyber security plan	Within 18 months of NRC approval of the cyber security plan.

References

- Bureau of Labor Statistics, Consumer Price Index (CPI) calculator, http://www.bls.gov/data/inflation_calculator.htm

- Department of Labor (U.S.), Bureau of Labor Statistics. Occupational Employment Statistics, Occupational Employment and Wages.

- Giesecke, J.A., et al., "Assessment of the Regional Economic Impacts of Catastrophic Events: CGE Analysis of Resource Loss and Behavioral Effects of an RDD Attack Scenario," *Risk Analysis*, Volume 32, Number 4, April 2012.

- Luna, Robert E., et al., "Survey of Costs Arising From Potential Radionuclide Scattering Events," SAND2008-0221C, Sandia National Laboratories, paper presented at the Waste Management Forum, Phoenix, AZ, February 24-28, 2008.

- Management Directive 12.2, "NRC Classified Information Security Program," U.S. Nuclear Regulatory Commission, Washington, DC, June 2014.

- NRC, "Draft Backfit Analysis and Documented Evaluation for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR 73.53)," U.S. Nuclear Regulatory Commission, Washington, DC, January 2017. (ADAMS Accession No. ML117018A221).

- NUREG/BR-0184, "Regulatory Analysis Technical Evaluation Handbook, Final Report," U.S. Nuclear Regulatory Commission, Washington, DC, January 1997.

- NUREG/BR-0058, "Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission," Revision 4, U.S. Nuclear Regulatory Commission, Washington, DC, September 2004.

- NUREG/CR-4627, "Generic Cost Estimates, Abstracts from Generic Studies for Use in Preparing Regulatory Impact Analyses," Revision 2, U.S. Nuclear Regulatory Commission, Washington, DC, February 1992.

- NUREG-1350, Vol.27, "NRC Information Digest, 2015-2016," U.S. Nuclear Regulatory Commission, Washington, DC, August 2015.

- OMB Circular No. A-4, "Regulatory Analysis," U.S. Office of Management and Budget, Washington, DC, September 17, 2003.

- OMB Circular A-76 "Performance of Commercial Activities," U.S. Office of Management and Budget, Washington, DC, May 29, 2003, as amended.

- OMB Circular A-94 "Guidelines and Discount Rates for Benefit-cost Analysis of Federal Programs," U.S. Office of Management and Budget, Washington, DC, October 29, 1992.

Appendix A: Estimated Operational Years Remaining for Fuel Cycle Facility Licensees

Name of Facility	Location	Status	License expiration date	Estimated closure date	Remaining estimated operational years*
American Centrifuge Plant***	Piketon, OH	License issued, construction halted	2037	2037	0
AREVA, Inc	Richland, WA	Active	2049	2049	31
Babcock & Wilcox Nuclear Operations Group	Lynchburg, VA	Active	2027	2027	9
Eagle Rock Enrichment Facility***	Idaho Falls, ID	License issued, construction not started	2041	2041	0
GE-Hitachi***	Wilmington, NC	License issued, construction not started	2052	2052	0
Global Nuclear Fuel – Americas, LLC	Wilmington, NC	Active	2049	2049	31
Honeywell International, Inc.	Metropolis, IL	Active	2017	2047	38
International Isotopes Fluorine Products, Inc.***	Lea County, NM	License issued, construction not started	2052	2052	0
Louisiana Energy Services, Urenco USA	Eunice, NM	Active	2040	2040	22
Nuclear Fuel Services	Erwin, TN	Active	2037	2037	19
Shaw AREVA MOX Services, LLC**	Aiken, SC	Under construction (operating license under review)	2044	2044	25
Westinghouse Electric Company, LLC	Columbia, SC	Active	2027	2047	29

* based on final rule going into effect in 2018
** estimated issuance of license in 2019
*** For the purpose of this analysis, this facility is not included because the NRC is not able to determine if, or when, the associated licensee would possess licensed material and, therefore, be subject to the provisions of the proposed rule.

Appendix B: Vulnerability of Fuel Cycle Facilities to a Cyber Threat

The U.S. Department of Homeland Security, Federal Bureau of Investigation, and the National Security Agency provide the NRC with periodic updates regarding the evolving cyber security threat. These briefings typically focus on the potential consequences that this threat poses to hardened (i.e., non-internet facing and protected against compromise) computer systems and networks. During NRC site visits at FCFs, the NRC staff observed potentially exploitable vulnerabilities in licensee computer systems, networks, and digital assets. Many of these systems, networks, and assets were not hardened. It is probable that the evolving cyber threat would have a greater impact on systems and networks that are not hardened.

As licensees implement digital upgrades for safety, security, and safeguards systems at their facilities, the potential for adverse consequences from a cyber attack will likely increase. The proposed cyber security rule would minimize the risk of a cyber attack causing a consequence of concern by requiring licensees to implement a comprehensive cyber security program. This would result in an increase in the overall safety and security of FCFs.

As discussed in Section 1.1, some FCF licensees are implementing voluntary cyber security measures to address cyber security vulnerabilities. The industry's voluntary initiative encouraged FCF licensees to independently consider: (1) formation of a cyber security assessment team; (2) training appropriate facility personnel; (3) establishing controls for portable media, devices, and equipment whose compromise could result in a high consequence event; and (4) establishing an incident response to a cyber attack and a recovery capability (for additional details, see the final regulatory basis). The NRC staff, based on its site visits at FCFs, has determined that the implementation of the voluntary cyber security measures varies greatly from facility to facility. The staff's observations indicate that the voluntary cyber security measures lack a comprehensive analysis of cyber security vulnerabilities and, in certain cases, only address a limited number of cyber security controls.

The Nature of Cyber Attacks

The U.S. Intelligence Community's 2016 Worldwide Threat Assessment highlighted the fact that systematic and persistent cyber security vulnerabilities in key sectors present adversaries with asymmetric opportunities. 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. Furthermore, a cyber attack does not need to be specifically directed at a FCF licensee to have an impact (e.g. malware exploiting a generic vulnerability). A cyber attack can come from any number of vectors – terror groups, hacktivists, nation states, or employees. A cyber attack allows an attacker to avoid exposure to a physical security force and/or the resultant potential radiological or chemical consequences of concern. Cyber attacks allow for repeated intrusion attempts without proximity to the licensee. The proposed rule would provide a substantial increase in the overall protection of the public health and safety and the common defense and security by requiring FCF licensees to establish, implement, and maintain a cyber security program to protect against cyber security threats.

Recent Cyber Attacks Affecting Industrial Control Systems Analogous to Those at FCFs

Recent cyber attacks have been designed to have physical consequences. This is illustrated by the: Stuxnet worm attack of 2010; Duqu malware of 2011; Havex malware of 2011; Flame

malware of 2012; physical effects from a cyber attack on a German steel mill in 2014; physical effects from a cyber attack on a water treatment facility in 2015 (estimated); and BlackEnergy malware causing the Ukrainian power outage in 2015. The global malware campaigns of Havex and BlackEnergy resulted in the perpetrator gaining access to unsecured industrial control systems that went unnoticed for years.

An analysis of the referenced cyber attacks from 2015 provides lessons that are applicable to FCF licensees. The systems attacked and the vulnerabilities exploited by the 2015 attacks are similar to the assets and vulnerabilities that the NRC staff identified during FCF site visits. Exploitation of these vulnerabilities at FCFs could result in consequences of concern.

One recent example was documented by Verizon Enterprise Solutions (VES), a division of Verizon Communications that provides services and products for Verizon's business and government clients around the world. VES was engaged by a water treatment facility (name withheld) regarding a possible breach of its computer systems as well as its process control network. VES reported details of this cyber attack in Scenario 8 of VES' 2016 Data Breach Digest (available online at http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf). As stated in the digest:

> More specifically, an unexplained pattern of valve and duct movements had occurred over the previous 60 days. These movements consisted of manipulating the Programmable Logic Controllers that managed the amount of chemicals used to treat the water to make it safe to drink, as well as affecting the water flow rate, causing disruptions with water distribution.

The digest also documented that the exploited process system existed on the same network as the water treatment facility's business applications and in part was housed on the same device. This condition created a pathway that the attackers exploited after finding an Internet facing business application that was vulnerable to compromise (i.e., its passwords were held in clear text and readable from the Internet). Gaining access to the business application and using the pathway allowed attackers to analyze and take control of the process network.

Based on its experience, VES detailed the following lessons learned:

- Having internet facing servers, especially web servers, directly connected to Supervisory Controls And Data Acquisition (SCADA) management systems is "far from a best practice;"
- Outdated systems and missing patches contributed to the data breach;
- Critical assets should be isolated;
- Weak authentication mechanisms and unsafe practices of protecting passwords also enabled the threat actors to gain far more access than should have been possible; and
- The water treatment facility's "alert functionality played a key role in detecting the changed amounts of chemicals and the flow rates."

In its final conclusion, VES stated that the "implementation of a layered defense-in-depth strategy could have detected the attack earlier, limiting its success or preventing it altogether." The VES lessons learned and final conclusion directly relate to similar vulnerabilities observed at FCFs by NRC staff during site visits in 2015. These observations have been documented in SECY-14-1047 (not publicly available due to security-related information), additional trip reports

(ADAMS Accession No. ML15314A621), and a more detailed document that has been designated as safeguards information.

Based on NRC staff observations, potential vulnerabilities at FCFs are similar to those exploited by the cyber attack on the water treatment facility (i.e., a cyber attack on a FCF licensee could allow an attacker to manipulate a given process by altering the process material or the flow control through the process). The end result would be a potential consequence of concern (e.g., criticality or chemical exposure).

The consequence described in the cyber attack on the water treatment facility is similar to that of an active consequence of concern described in the proposed rule. An active consequence of concern would involve the compromise of similar digital assets (e.g., industrial control systems, process control networks, and SCADA systems). Given that similar conditions exist in both the water treatment facility and at FCFs overall, the NRC staff has concluded that the active consequence of concern is a viable result of a cyber attack against a FCF licensee. Furthermore, ensuring that FCF licensees establish, implement, and maintain a cyber security program to detect, protect against, and respond to a cyber attack capable of causing an active consequence of concern, correlates to the lessons learned from the referenced cyber attack on the water treatment facility, and would provide an increase in the protection of health and safety at FCFs.

A second example involves the physical consequences resulting from a cyber attack of several regional electrical transmission organizations called Oblenergos in the Ukraine during December 2015. This was a multilayered cyber attack resulting in the shutdown of several transmission substations and the loss of power for an estimated 225,000 customers for several hours. As detailed in the report, "Analysis of the Cyber Attack on the Ukrainian Power Grid" prepared by SANS Institute (see https://www.sans.org) and published by the Electricity Information Sharing and Analysis Center (available online at https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf), the unauthorized control of the transmission systems event involved an initial spear phishing email campaign, followed by the installation of malware to harvest credentials, and then, after learning how to control certain industrial control systems, concluded with a separate cyber attack (i.e., initiating event).

Under normal operating conditions, these utilities had the ability to remotely control and reset their transmission substations. As a part of the actual attack, the associated communication channels were severed. The attackers used malware to damage the firmware of the devices used to remotely communicate with the substations. In addition, they sent malware to wipe the computers used by utility staff to control the substations. Thus when workers saw that the substations had failed, they were unable to remotely restart the systems and had to physically travel to each site. This hampered their immediate response efforts and had the net effect of extending the blackout for customers.

The report lists several recommended actions to protect against future cyber attacks against electrical utilities. These include:

- Properly segment networks from each other and ensure logging is enabled on devices that support it;
- Enforce a password reset policy in the event of a compromise;
- Utilize up-to-date antivirus or endpoint security technologies to allow for the denial of

known malware;
- Continuously perform network security monitoring for abnormalities; and
- Plan and train to incident response plans that incorporate appropriate personnel.

Analogous to the communication pathways in the cyber attack described above, FCF licensees utilize similar configurations with certain digital assets that are relied on for safety (e.g., a digital pressure relief valve with an external communications pathway). Furthermore, similar vulnerabilities (e.g., lack of network segmentation or isolation, lack of intrusion detection capabilities, lack of time of use restrictions for remote users) identified in the subject cyber attack are congruent with the vulnerabilities observed by the NRC staff during site visits at FCFs. Therefore, it can be extrapolated that the conditions that caused disruptions to response efforts by the transmission utility staff could similarly exist for FCF licensees as the result of a cyber attack. This demonstrates that under similar conditions, a cyber attack at a FCF could result in a latent consequence of concern.

Given the evolving nature of cyber attacks and the growth in cyber threat vectors, as well as the lessons learned from recent real world cyber attacks on industrial control systems, the NRC staff has determined that there are potentially exploitable cyber security vulnerabilities at FCFs. Exploitation of these vulnerabilities as demonstrated by the real world examples presented, could result in a consequence of concern impacting public health and safety or the common defense and security.

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

RIN number: 3150-AJ64

NRC Docket ID: NRC-2015-0179

2017

INTRODUCTION

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

HISTORICAL BACKGROUND AND OVERVIEW

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

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

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

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

ENVIRONMENTAL ASSESSMENT

I. Identification of the Proposed Action

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

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

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

II. Need for the Action

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

III. Alternatives to the Proposed Action

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

Alternative 1: No Action

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

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

Other Approaches Considered

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

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

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

Summary of Alternatives to the Proposed Action

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

Environmental Impacts of the Proposed Action and Alternative

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

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

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

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

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

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

Environmental Impacts of Alternatives to the Proposed Action

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

IV. Agencies and Persons Consulted

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

FINDING OF NO SIGNIFICANT IMPACT

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

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

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