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

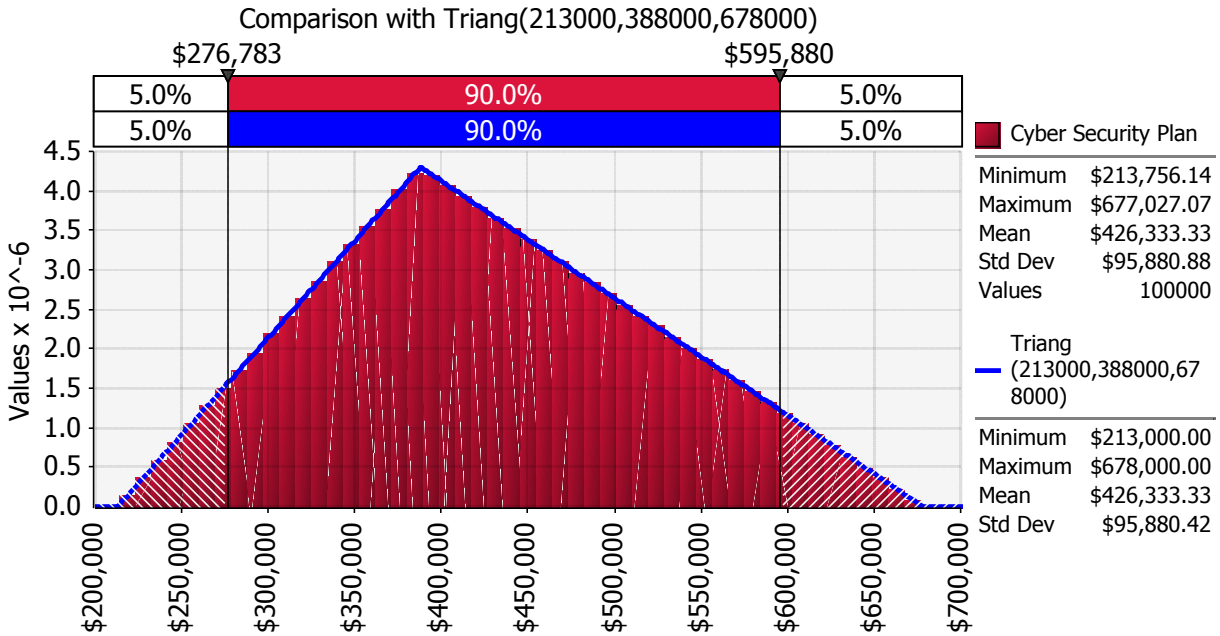


Figure 5-2 Analysis of Digital Assets

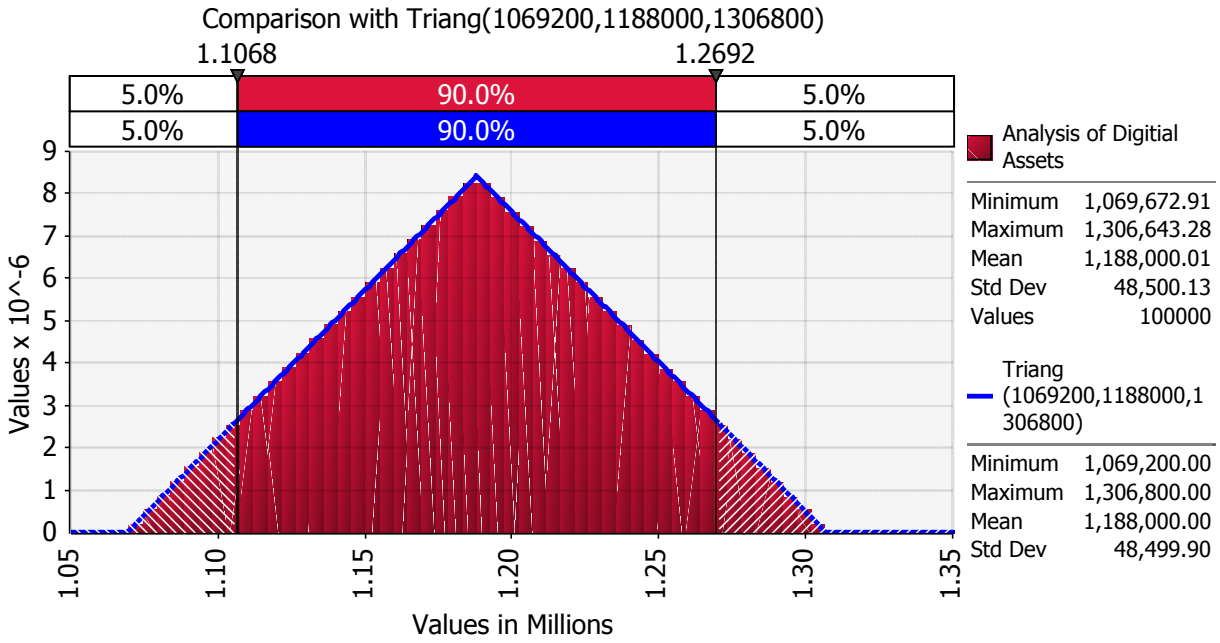


Figure 5-3 Cyber Security Controls

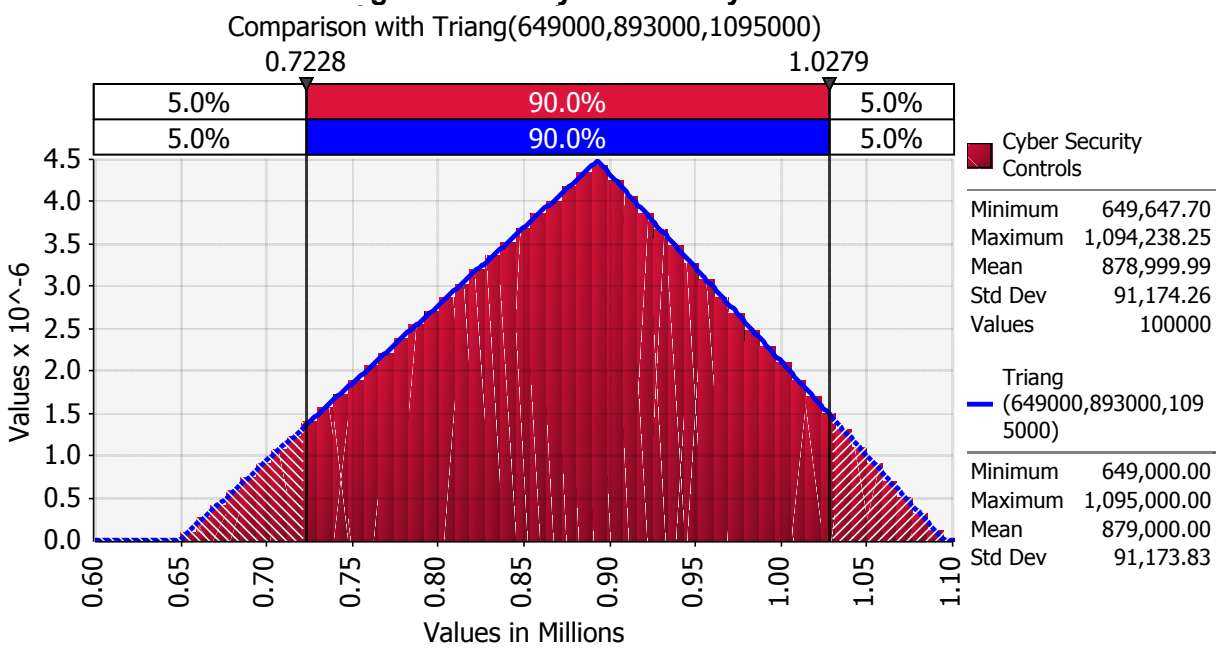
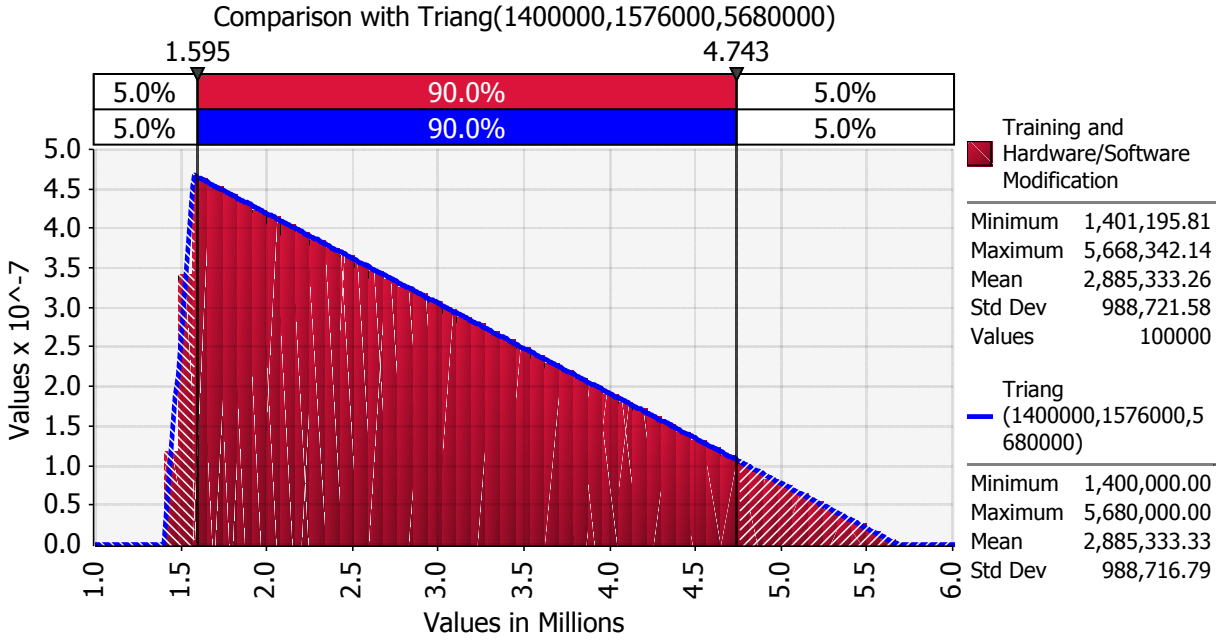


Figure 5-4 Training and Hardware or Software Modification



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.