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

U.S. Nuclear Regulatory Commission

Office of Nuclear Material Safety and Safeguards

2017

TABLE OF CONTENTS

LIST OF TABLES iii

ABBREVIATIONS AND ACRONYMS iv

I. INTRODUCTION 5

I.1 Background 5
I.2 Backfit requirements 7
I.3 Existing requirements 8
I.4 Proposed requirements for cyber security at fuel cycle facilities 10
I.5 Entities subject to backfit protection 13
I.6 Considerations of backfit for existing facilities 14

II. PROPOSED REQUIREMENTS THAT DO NOT CONSTITUTE BACKFITTING 21

III. EXCEPTIONS TO BACKFIT ANALYSIS 22

III.1 Why are certain cyber security requirements needed now for adequate protection? 22
III.2 Proposed DBT requirements necessary for adequate protection 23
III.3 Proposed classified information requirements necessary for adequate protection 25
III.4 Sections of the proposed rule required for adequate protection 26
III.5 Conclusion 31

IV. BACKFIT ANALYSIS: SUBSTANTIAL INCREASE IN OVERALL PROTECTION 32

IV.1 Finding of a substantial increase in overall protection of public health and safety 33
IV.2 Section-by-section analysis for substantial increase in overall protection 34
IV.3 Section-by-section analysis 34
IV.4 Conclusion 39

V. BACKFIT ANALYSIS: COST JUSTIFICATION 40

V.1 Costs 40
V.2 Implementation costs 41
V.3 Annual operational costs 43
V.4 Summary of estimated costs for the substantial increase in overall protection 46
V.5 Benefits 46

VI. OTHER FACTORS FOR CONSIDERATION IN THE BACKFIT ANALYSIS 56

VII. OVERALL CONCLUSION 62

REFERENCES 63

LIST OF TABLES

Table I-1 Facilities subject to the proposed requirements in 10 CFR 73.53 6
Table I-2 Percentage of costs estimated to implement proposed requirements necessary for adequate protection versus those subject to a backfit analysis 16
Table I-3 Breakdown of how costs are considered in the backfit analysis 20
Table IV-1 Summary of averted cost per single event 33
Table V-1 Costs necessary for the substantial increase in overall protection 46
Table V-2 Averted cost per minimum event – radiological exposure 50
Table V-3 Averted cost per maximum event – radiological exposure 50
Table V-4 Averted cost per minimum event – intake of 30 mg or greater of uranium in soluble form outside the controlled area 51
Table V-5 Averted cost per maximum event – intake of 30 mg or greater of uranium in soluble form outside the controlled area 51
Table V-6 Averted cost per minimum event – acute chemical exposure 52
Table V-7 Averted cost per maximum event – acute chemical exposure 53
Table V-8 Summary of averted cost per single event 53
Table V-9 Cost beneficial event frequency and magnitude 54
Table VI-1 NRC implementation cost 59
Table VI-2 NRC annual cost 60

ABBREVIATIONS AND ACRONYMS

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

I. INTRODUCTION

I.1 Background

The U.S. Nuclear Regulatory Commission (NRC) is proposing to amend Title 10 of the *Code of Federal Regulations* (10 CFR) Part 73, "Physical Protection of Plants and Materials," to establish cyber security requirements for certain nuclear fuel cycle facility (FCF) applicants and licensees. The proposed regulation, if approved, would require FCF applicants and licensees within the scope of the rule to establish, implement, and maintain a cyber security program designed to promote common defense and security and to provide reasonable assurance that the public health and safety remain adequately protected against the evolving risk of cyber attacks. The proposed requirements, if approved, would apply to each FCF applicant and licensee that is authorized or requests authorization to: (1) possess greater than a critical mass of special nuclear material (SNM) and engage in enriched uranium processing, fabrication of uranium fuel or fuel assemblies, uranium enrichment, enriched uranium hexafluoride conversion, plutonium processing, fabrication of mixed-oxide fuel or fuel assemblies, scrap recovery of SNM, or any other FCF activity that the Commission determines could significantly affect public health and safety; or (2) engage in uranium hexafluoride conversion or uranium hexafluoride deconversion. As such, the proposed requirements would apply to each FCF applicant and licensee subject to the requirements of 10 CFR 70.60, "Applicability," and to each applicant or licensee subject to the requirements of 10 CFR Part 40, "Domestic Licensing of Source Material," for the operation of a uranium hexafluoride conversion or deconversion facility. Hereafter, the FCF applicants and licensees to which the proposed rule would be applicable will be referred to as "FCF licensees."

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

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

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

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

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

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

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

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

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

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

I.2 Backfit requirements

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

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

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

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

I.3 Existing requirements

The NRC currently lacks a comprehensive regulatory framework for addressing cyber security at FCFs. Subsequent to the events of September 11, 2001, the NRC issued Interim Compensatory Measure (ICM) Orders that required FCF licensees to evaluate computer and communications networks and address safety and security vulnerabilities as necessary. However, the NRC did not provide guidance on how to implement the cyber security requirement in the ICM Orders. Additionally, in Section 651 of the Energy Policy Act of 2005, Congress directed the Commission to initiate a rulemaking to revise the design basis threats (DBTs) set forth in 10 CFR 73.1, "Purpose and scope." The Commission was specifically directed to consider a potential cyber threat in the DBT rulemaking. In 2007, in response to this direction, the Commission promulgated a rulemaking entitled "Design Basis Threat" (72 FR 12705; dated March 19, 2007), revising 10 CFR 73.1 to explicitly include a cyber security threat as an element of the DBTs.

In accordance with 10 CFR 73.20, "General performance objective and requirements," Category I FCF licensees must maintain a physical protection system designed to protect against both the DBT for radiological sabotage and the DBT for theft or diversion of formula quantities of SSNM. Both DBTs include a cyber attack as a method that may be exploited by adversaries. However, current NRC physical protection requirements do not set forth specific provisions for addressing cyber attacks at Category I FCFs. Furthermore, no NRC guidance specifically discusses requirements or strategies for protecting against cyber attacks for FCFs.

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

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

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

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

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

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

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

The proposed 10 CFR 73.53(b), "Cyber security program performance objectives," would require FCF licensees to establish, implement, and maintain a cyber security program to detect, protect against, and respond to a cyber attack capable of causing one or more of the consequences of concern identified in 10 CFR 75.53(c), "Consequences of concern."

I.4.1 Consequences of Concern

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

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

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

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

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

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

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

The distinction between active and latent consequences of concern is that, in the case of an active consequence of concern, the compromise of the digital asset from a cyber attack directly results in a radiological or chemical exposure exceeding the proposed regulatory thresholds. In the case of a latent consequence of concern, a digital asset is compromised but there is no direct impact on a safety, security, or safeguards function until a secondary event occurs (i.e., an initiating event separate from the cyber attack). When there is a latent consequence of concern, the compromised digital asset is no longer available to provide the function needed to prevent the secondary event. The compromise of the digital asset from the cyber attack (i.e., the latent consequence of

concern) and the secondary event must both occur for there to be a significant impact on public health and safety or the common defense and security.

I.4.2 Cyber Security Program

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

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

b. The proposed 10 CFR 73.53(d)(2) would require FCF licensees to establish and maintain cyber security controls that provide performance specifications to detect, protect against, and respond to a cyber attack capable of causing a consequence of concern. The cyber security controls would prevent the types of consequences of concern specific to the facility, as specified in 10 CFR 73.53(c).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

I.5 Entities subject to backfit protection

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

I.5.1 Conversion and Deconversion facility licensees

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

I.5.2 Part 70 FCF licensees

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

I.6 Considerations of backfit for existing facilities

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Cost Allocation

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

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

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

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

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

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

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

II. PROPOSED REQUIREMENTS THAT DO NOT CONSTITUTE BACKFITTING

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

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

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

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

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

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

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

III. EXCEPTIONS TO BACKFIT ANALYSIS

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

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

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

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

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

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

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

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

III.2 Proposed DBT requirements necessary for adequate protection

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

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

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

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

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

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

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

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

III.3 Proposed classified information requirements necessary for adequate protection

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

III.5 Conclusion

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

IV. BACKFIT ANALYSIS: SUBSTANTIAL INCREASE IN OVERALL PROTECTION

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

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

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

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

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

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

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

active safety or latent safety consequence of concern.

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

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

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

Table IV-1 Summary of averted cost per single event

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

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

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

increase in overall protection of public health and safety.

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

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

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

IV.3 Section-by-section analysis

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IV.4 Conclusion

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

V. BACKFIT ANALYSIS: COST JUSTIFICATION

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

V.1 Costs

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

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

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

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

V.2 Implementation costs

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The total costs are calculated as follows:

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

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

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

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

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

The total costs are calculated as follows:

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

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

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

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

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

The total costs are calculated as follows:

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

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

V.3 Annual operational costs

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

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

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

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

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

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

The total annual costs are calculated as follows:

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

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

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

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

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

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

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

The total annual costs are calculated as follows:

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

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

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

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

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

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

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

The total annual costs are calculated as follows:

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

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

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

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

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

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

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

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

V.5 Benefits

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

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

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

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

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

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

variability in existing cyber security programs at FCFs.

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

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

V.5.1.1 Methodology

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

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

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

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

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

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

consequence of concern.

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

- exposure of 0.25 Sv (25 rem) or greater for any individual (i.e., worker or member of the public);

- intake of 30 mg or greater of uranium in soluble form for any individual outside the controlled area (i.e., member of public); or

- acute chemical exposure that could lead to irreversible or other serious, long-lasting health effects for any individual (i.e., worker or member of the public).

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

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

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

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

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

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

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

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

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

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

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

[4] 2010 Census data.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

V.5.1.5 Analysis Conclusions

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

Table V-8 Summary of averted cost per single event

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

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

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

Table V-9 Cost beneficial event frequency and magnitude

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

[a] Event does not consider additional cost of clean-up or decontamination
[b] The acronym "exp." stands for exposure per individual
[c] The radiological exposure could be distributed among up to 10 people (e.g., number considered for the bounding radiological exposure)

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

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

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

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

V.5.2 Qualitative Benefits

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

V.5.2.1 Improvements in Knowledge

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

V.5.2.2 Regulatory Efficiency

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

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

V.5.2.3 Improved Reliability and Public Confidence

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

V.5.3 The Proposed Rule Is Cost Justified

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

VI. OTHER FACTORS FOR CONSIDERATION IN THE BACKFIT ANALYSIS

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

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

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

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

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

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

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

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

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

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

Installation and Continuing Costs

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

Potential Impact of Facility Downtime

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

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

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

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

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

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

Implementation Burden

Rulemaking

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

Create inspection procedures and training

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

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

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

Table VI-1 NRC implementation cost

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

NRC Operations Burden

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

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

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

Table VI-2 NRC annual cost

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

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

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

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

See Section VI of this backfit analysis.

Potential Impact of Differences in Facility Type

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

Potential Impact of Differences in Design

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

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

Potential Impact of Differences in Age

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

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

The backfit is final.

Backfitting should be required

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

VII. OVERALL CONCLUSION

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

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

REFERENCES

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

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

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

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

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

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

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

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

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

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

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

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