

Rulemaking for Cyber Security at Fuel Cycle Facilities

RIN number: 3150-AJ64

NRC Docket ID: NRC-2015-0179

Regulatory Basis Document



2016

Table of Contents

Abbreviations and Acronyms	v
Chapter 1 Introduction and Background	1-1
Chapter 2 History and Existing Regulatory Framework	2-1
2.1 History	2-1
2.1.1 Post 9/11 Security Orders: 2001-2006	2-1
2.1.2 Design Basis Threat Rulemaking	2-1
2.1.3 Power Reactor Regulatory Requirements, 10 CFR 73.54: 2009-2012.....	2-2
2.1.4 Cyber Security Roadmap: 2012.....	2-3
2.1.5 Fuel Cycle Cyber Security Working Group – Initial Review: 2010-2013.....	2-3
2.1.6 Fuel Cycle Cyber Security Working Group – Options for Commission: SECY-14-0147 and the SRM to SECY-14-0147	2-5
2.1.7 Related Publications	2-7
2.2 Existing Fuel Cycle Cyber Security Regulatory Framework.....	2-8
2.2.1 NRC Security Orders	2-8
2.2.2 NRC Regulations	2-8
2.2.3 NRC Voluntary Reporting Criteria.....	2-10
2.2.4 Other Federal Laws and Regulations Addressing Cyber Security.....	2-11
2.2.5 Other Federal Agencies Involved in Cyber Security	2-12
2.3 NRC Authority for Rulemaking.....	2-12
2.4 Summary.....	2-13
Chapter 3 Regulatory Problem.....	3-1
3.1 Cyber Security Threats and Attack Vectors	3-1
3.2 Vulnerabilities and Pathways	3-4
3.3 Lack of Robust and Comprehensive Regulatory Framework	3-5
3.4 Potential Consequences	3-9
3.4.1 Safety.....	3-10
3.4.2 Security.....	3-11
3.4.3 Emergency Preparedness	3-11
3.4.4 MC&A	3-11
3.5 Summary.....	3-12
Chapter 4 Basis for Requested Change	4-1
4.1 Commission Direction	4-1
4.2 Proposed Changes	4-1
4.3 Technical Approach	4-2
4.4 Resolution	4-5
4.4.1 Formation of a CST	4-5
4.4.2 Training staff on cyber security.....	4-6
4.4.3 Identification of digital assets associated with 3S functions.....	4-6
4.4.4 Application of cyber security controls to digital assets.....	4-10
4.4.5 Configuration management	4-10
4.4.6 Cyber security incident response capability.....	4-11
4.4.7 Cyber security event reporting and recordkeeping	4-11
4.5 Summary.....	4-11

Chapter 5 Alternatives to Rulemaking Considered	5-1
5.1 No Action	5-1
5.1.1 Timing and Resources	5-1
5.1.2 Stakeholder Interactions	5-1
5.1.3 Regulatory Stability and Enforceability	5-1
5.1.4 Summary	5-2
5.2 Issue Cyber Security Orders	5-2
5.2.1 Timing and Resources	5-2
5.2.2 Stakeholder Interactions	5-3
5.2.3 Regulatory Stability and Enforceability	5-3
5.2.4 Summary	5-4
5.3 Issue Generic Communications	5-4
5.3.1 Timing and Resources	5-4
5.3.2 Stakeholder Interactions	5-4
5.3.3 Regulatory Stability and Enforceability	5-5
5.3.4 Summary	5-5
5.4 Develop Regulatory Guidance Documents	5-5
5.4.1 Timing and Resources	5-5
5.4.2 Stakeholder Interactions	5-5
5.4.3 Regulatory Stability and Enforceability	5-5
5.4.4 Summary	5-6
5.5 Issue Site-Specific License Conditions	5-6
5.5.1 Timing and Resources	5-6
5.5.2 Stakeholder Interactions	5-6
5.5.3 Regulatory Stability and Enforceability	5-7
5.5.4 Summary	5-7
5.6 Clarify Inspection Modules / Revise Enforcement Guidance	5-7
5.7 Summary	5-7
Chapter 6 Backfit Rule Applicability	6-1
6.1 Entities Accorded Backfit Protection	6-1
6.2 Future Applicants	6-1
6.3 10 CFR Part 40 Facilities	6-2
6.4 10 CFR Part 70 Facilities	6-2
6.4.1 Backfitting Defined	6-2
6.4.2 Administrative Changes which are Not Subject to Backfit Considerations	6-2
6.4.3 Information Collection and Reporting	6-2
6.4.4 Codification of Requirements in Orders	6-3
6.4.5 Requirements Not Falling into Any Category of Backfitting Rationales	6-3
Chapter 7 Stakeholder Interactions	7-1
7.1 Overview	7-1
7.2 NRC Public Meetings Specific to the Regulatory Basis	7-2
7.3 Comments on the Draft Regulatory Basis	7-2
Chapter 8 Cost/Impact Considerations	8-1
8.1 Applicability	8-1
8.2 Potential Licensee Impacts	8-1
8.2.1 Establish a Cyber Security Program	8-1

8.2.2	Maintenance and Configuration Management.....	8-2
8.2.3	Documentation and Event Reporting.....	8-2
8.2.4	Additional Considerations for Licensees.....	8-2
8.3	Impact on the NRC	8-3
8.3.1	Rulemaking.....	8-3
8.3.2	NRC Oversight.....	8-3
8.4	Impact on State, Local, or Tribal Governments	8-3
8.5	Environmental Analysis.....	8-4
8.6	Cost Justification.....	8-4
Chapter 9 NRC Strategic Plan		9-1
Chapter 10 Guidance Documents.....		10-1
10.1	New Guidance Documents	10-1
10.2	Existing Guidance Documents to be Revised.....	10-1
10.3	Rescinded Guidance Documents	10-1
10.4	Inspection Program.....	10-1
Chapter 11 Resources		11-1
Chapter 12 Timing.....		12-1
Chapter 13 References		13-1
Attachment A. Outreach Initiatives for Fuel Cycle Cyber Security		A-1

Abbreviations and Acronyms

3S	safety, security, and safeguards
ADAMS	Agencywide Documents Access and Management System
AEA	Atomic Energy Act of 1954, as amended
CFR	<i>Code of Federal Regulations</i>
CSP	Cyber Security Program, U.S. Department of Energy
CST	cyber/computer security team
DBT	design basis threat
DHS	U.S. Department of Homeland Security
DOD	U.S. Department of Defense
DOE	U.S. Department of Energy
EO	Executive Order
EP	emergency preparedness
EPAct	Energy Policy Act of 2005
FCF	nuclear fuel cycle facility
FISMA	Federal Information Security Management Act
FNMC	fundamental nuclear material control
FR	<i>Federal Register</i>
IA	Information Assessment
IAEA	International Atomic Energy Agency
ICM	interim compensatory measures
ICS	industrial control system
ICS-CERT	Industrial Control Systems – Cyber Emergency Response Team of the U.S. Department of Homeland Security
INFCIRC	Information Circulars
INFOSEC	information security
IROFS	item(s) relied on for safety
ISA	integrated safety analysis
MC&A	material control and accounting
NEI	Nuclear Energy Institute
NIST	U.S. National Institute of Standards and Technology
NRC	U.S. Nuclear Regulatory Commission
NSI	national security information
PCN	process control network
PFAPS	plant features and procedures
PMDE	portable media devices and equipment

RD	restricted data
RG	Regulatory Guide
SECY	Secretary of the Commission, Office of the U.S. Nuclear Regulatory Commission
SGI	safeguards information
SNM	special nuclear material
SP	Special Publication
SRM	staff requirements memorandum
SSEPMCA	safety, security, emergency preparedness, and material control & accounting
SSNM	strategic special nuclear material
USB	universal serial bus

Chapter 1 Introduction and Background

The U.S. Nuclear Regulatory Commission (NRC) is initiating this rulemaking to establish new cyber security regulations in Part 73 of Title 10 of the *Code of Federal Regulations* (10 CFR), “Physical Protection of Plants and Materials.” The objective of this rulemaking is to develop and issue new regulatory requirements for nuclear fuel cycle facility (FCF) licensees. FCF licensees include those licensed under: (1) 10 CFR Part 70 and authorized to possess or use a formula quantity of strategic special nuclear material (SSNM) as defined in 10 CFR 73.2 (hereafter referred to as Category I facilities); (2) 10 CFR Part 70 and authorized to possess or use special nuclear material (SNM) of moderate strategic significance as defined in 10 CFR 73.2 (hereafter referred to as Category II facilities); (3) 10 CFR Part 70 and authorized to possess or use SNM of low strategic significance as defined in 10 CFR 73.2 (hereafter referred to as Category III facilities); and (4) 10 CFR Part 40 and authorized to operate as conversion/deconversion facilities. These licensees would be required to establish and maintain a cyber security program that implements a graded, performance-based regulatory framework for the protection of digital computer systems, communication systems, and networks associated with safety, security (physical and information), and safeguards (3S) functions from cyber attacks that could result in one of the following consequences of concern:

- significant exposure events that could endanger the life of workers or could lead to irreversible or other serious, long-lasting health effects to workers or members of the public (e.g., nuclear criticalities and releases of radioactive materials or chemicals) [safety];
- radiological sabotage and theft or diversion of formula quantities of SSNM [security – limited to Category I facilities];
- loss of control and accounting of formula quantities of SSNM [security & safeguards – limited to Category I facilities];
- unauthorized removal of SNM of moderate strategic significance [security – limited to Category I and II facilities];
- loss of control and accounting of SNM of moderate strategic significance [security & safeguards – limited to Category I and II facilities]; or
- loss or unauthorized disclosure of classified information [security].

In the staff requirements memorandum (SRM) to SECY-14-0147, “Cyber Security for Fuel Cycle Facilities,” dated March 24, 2015 (Accession No. ML15083A175 in the NRC’s Agencywide Documents Access and Management System (ADAMS)), the Commission disapproved the staff’s recommendation to issue security orders to FCF licensees followed by a rulemaking for cyber security. However, the SRM to SECY-14-0147 approved initiation of a high-priority rulemaking to develop cyber security requirements for FCF licensees and further stated that the final rule should be completed and implemented in an expeditious manner.

This rulemaking would require FCF licensees to establish appropriate levels of protection against cyber attacks that could result in a consequence of concern based on the facility type

(i.e., Category I, II, III, or 10 CFR Part 40 conversion/deconversion facilities). The facility type approach to implementing specific cyber security controls is further discussed in Chapter 4 of this document.

A cyber attack is defined as the manifestation of physical, electronic, or digital threats against computers, communication systems, or networks that may: (1) originate from either inside or outside the licensee's facility, (2) utilize internal and/or external components, (3) involve physical, electronic, or digital threats, (4) be directed or non-directed in nature, (5) be conducted by threat agents having either malicious or non-malicious intent, and (6) have the potential to result in a consequence of concern. Cyber attacks, consequences of concern, and the need for this rulemaking are discussed in greater detail in Chapter 3 of this document.

The scope of this regulatory basis includes cyber security for Category I, II, and III FCFs licensed under 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material," and uranium hexafluoride conversion and deconversion facilities licensed under 10 CFR Part 40, "Domestic Licensing of Source Material." Each of these licensee types (e.g., conversion, enrichment, fuel fabrication, etc.) has potential consequences of concern that are unique to their respective facilities. To account for these differences, the staff plans to develop a graded, consequence-based approach for the identification and protection of digital assets at these various types of facilities.

The scope of this regulatory basis does not include cyber security for power reactors, non-power reactors, independent spent fuel storage installations, or byproduct material licensees. Power reactor licensees and combined license applicants have an established rule for cyber security in 10 CFR 73.54. SECY-12-0088, "The Nuclear Regulatory Commission Cyber Security Roadmap" (ADAMS Accession No. ML12135A050), discusses potential paths forward for each of the other licensee types independent of this regulatory basis.

Chapter 2 History and Existing Regulatory Framework

This chapter discusses the history of how the NRC has addressed cyber security for FCF licensees for activities involving source material, SNM, and hazardous chemicals regulated by the NRC. It also discusses the existing regulatory framework for addressing cyber security for these licensees. Discussion is provided on security orders, regulations, guidance, and licensee implemented voluntary actions. Additionally, this chapter provides the basis for the NRC staff's assessment that the existing regulatory framework is not adequate to address cyber security for FCF licensees.

2.1 History

In recent years, the threat of cyber attacks has steadily risen, both globally and nationally. The U.S. Government has observed an increase in: (1) the number of cyber attacks; (2) the level of sophistication of such attacks; and (3) the potential of these attacks to impact numerous digital assets, including digital assets at FCF licensees. Additionally, these attacks¹ can be conducted remotely from anywhere in the world.

2.1.1 Post 9/11 Security Orders: 2001-2006

In response to the terrorist attacks of September 11, 2001, the NRC issued a series of security orders to prevent certain potential consequences from a physical attack on FCF licensees. These orders addressed the threat environment at that time by imposing additional security requirements beyond the existing requirements in 10 CFR 73.20, 73.40, 73.45, 73.46, and 73.67. The NRC also issued a separate security order to certain FCF licensees governing the protection of certain radiological and hazardous chemicals at their facilities. In addition to physical security requirements, the Interim Compensatory Measures (ICM) Orders issued to FCF licensees in 2002 and 2003 contained a generic cyber security measure directing licensed facilities to evaluate and address cyber security vulnerabilities. This generic cyber security measure did not specify or provide guidance on the type of cyber security protection measures (e.g., intrusion detection) to employ or provide direction or guidance on the establishment of a formal cyber security program at FCF licensees. Furthermore, the orders provided limited guidance on implementation of the generic cyber security measure, focusing on computer systems that conduct and maintain communications during emergency response actions.

2.1.2 Design Basis Threat Rulemaking

Section 651 of the Energy Policy Act of 2005 (EPAAct) directed the Commission to initiate a rulemaking to revise the design basis threats (DBTs) set forth in 10 CFR 73.1. The Commission was further directed to consider, at a minimum, 12 factors when developing the DBT rulemaking, 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.

¹ An example of a cyber attack targeting an FCF was the Stuxnet worm launched against a uranium enrichment facility in Iran.

The DBTs are based on realistic assessments of the tactics, techniques, and procedures used by international and domestic terrorist groups, organizations and individuals. The DBTs describe general adversary characteristics that designated licensees, including Category I FCF licensees, must defend against with high assurance. These requirements include protection against radiological sabotage (generally applied to power reactors and Category I FCF licensees) and theft or diversion of NRC-licensed SSNM (generally applied to Category I FCF licensees). The DBTs are used by licensees to form the basis for site-specific defensive strategies. Furthermore, Regulatory Guide (RG) 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" (not in ADAMS and not publicly available because it contains safeguards information), was developed as an acceptable method for meeting the requirements of 10 CFR 73.1 for Category I FCF licensees. This RG provides guidance on the types of systems licensees should protect from cyber attacks but does not provide specific cyber security protection measures (controls) for licensees to implement.

2.1.3 Power Reactor Regulatory Requirements, 10 CFR 73.54: 2009-2012

In March 2009, the NRC further addressed cyber security during publication of the Power Reactor Security Requirements final rule (74 FR 13926). The cyber security requirements for power reactors were placed into a stand-alone section in 10 CFR 73.54, which require power reactors to provide high assurance that digital computer and communication systems and networks associated with nuclear power plant safety, security, and emergency preparedness (EP) functions are protected from cyber attacks. The development of associated guidance for implementing the requirements in 10 CFR 73.54 resulted in the publication of RG 5.71, "Cyber Security Programs for Nuclear Facilities" (ADAMS Accession No. ML090340159). RG 5.71 was developed for nuclear power plants and is based on cyber security standards and practices published by the National Institute of Standards and Technology (NIST). RG 5.71 also contains a generic template that power reactor licensees and combined license applicants may use as guidance in developing their required cyber security plans. The experience gained in developing this rule and its associated guidance informs the NRC staff's approach for developing similar cyber security requirements for other categories of licensees.

The NRC staff plans to apply lessons learned from the implementation of 10 CFR 73.54 to the rulemaking process for FCF licensees. These lessons learned include:

- Define a process for identifying digital assets/systems that are within the scope of the regulatory requirements that is specific and consequence-based.
- Establish a risk-informed screening process to identify in-scope digital assets that can have an equivalent function provided by an alternate means and therefore not require additional cyber security controls.
- Add flexibility within the rule language to allow licensees to satisfy the security objective by:
 - tailoring cyber security controls to account for system functionality/capability, and
 - taking credit for existing programs and alternate controls that perform equivalent functions.
- Ensure licensee programs and processes meet regulatory requirements prior to focusing on technical implementation.
- Potentially reducing the focus on the implementation of specific cyber security controls by considering the management of the overall risk through a process similar to NIST Special Publication (SP) 800-37, Rev. 1, “Applying a Risk Management Framework,” which allows the use of both qualitative and/or quantitative risk methodologies.
- Establishing an implementation schedule with firm deadlines.

2.1.4 Cyber Security Roadmap: 2012

In June 2012, the NRC staff completed SECY-12-0088, which established the NRC staff’s approach for evaluating the need for cyber security requirements for the following four categories of NRC licensees and facilities: (1) FCFs, (2) non-power reactors, (3) independent spent fuel storage installations, and (4) byproduct materials licensees. The roadmap reflects a graded approach to developing cyber security requirements commensurate with the inherent nuclear safety and security risks associated with the different types of licensees and facilities. Additionally, this roadmap aligns with the current NRC Strategic Plan, NUREG-1614, Volume 6, “Strategic Plan: Fiscal Years 2014-2018” (ADAMS Accession No. ML14246A439), which states that the NRC will evaluate the need for cyber security requirements for fuel cycle facilities.

2.1.5 Fuel Cycle Cyber Security Working Group – Initial Review: 2010-2013

Building on the experience gained through the establishment of the NRC’s regulatory framework for cyber security at nuclear power reactors, the NRC established a cyber security working group (working group) in 2010 consisting of staff from the Office of Nuclear Material Safety and Safeguards and the Office of Nuclear Security and Incident Response. The working group reviewed cyber security measures currently in place at FCF licensees to determine how these facilities protect their digital assets from cyber attacks and whether the NRC should take additional action to have FCF licensees strengthen their programs. The working group specifically looked at digital assets performing, supporting, or associated with critical functions, such as safety, security, emergency preparedness, and material control & accounting

(SSEPMCA), which if compromised, could impact public health and safety or common defense and security.

The working group determined that guidance used during the development of the power reactor cyber security requirements, specifically previous editions of the current NIST SP 800-53, Revision (Rev.) 4, "Security and Privacy Controls for Federal Information Systems and Organizations," was an appropriate benchmark to evaluate cyber security for FCF licensees. NIST SP 800-53, Rev. 4, provides a catalog of security and privacy controls for Federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the United States from a diverse set of threats including cyber attacks, natural disasters, structural failures, and human errors. The controls address a diverse set of security and privacy requirements derived from legislation, Executive Orders (EOs), policies, directives, regulations, standards, and/or mission/business needs for both the Federal government and the Nation's critical infrastructure. The publication also describes how to develop specialized sets of controls, or overlays, tailored for specific types of missions/business functions, technologies, or environments of operation. Finally, the catalog of security controls addresses security from both a functionality perspective (the strength of security functions and mechanisms provided) and an assurance perspective (the measures of confidence achieved from the implemented security capability). The approach in NIST SP 800-53, Rev. 4, to address both security functionality and security assurance, ensures that information technology products and the information systems built from those products using sound systems and security engineering principles are sufficiently trustworthy. The working group recognized that other nationally recognized standards may provide an equivalent level of protection as NIST SP 800-53, Rev. 4 (e.g., International Organization for Standardization and International Electrotechnical Commission 27000 series standards, U.S. Department of Energy (DOE) standards, and U.S. Department of Defense (DOD) standards).

The working group designed a four-step assessment process to examine cyber security for FCF licensees that included the following:

1. requesting FCF licensees to respond to an NRC questionnaire regarding the extent to which digital assets were used for SSEPMCA functions;
2. performing site visits to a representative cross section of FCF licensees;
3. analyzing licensees' documentation of their cyber security actions and observing how the programs were implemented; and
4. issuing a final report (not publicly available because it contains security-related information, ADAMS Accession No. ML120900705).

The final report issued by the working group discusses NRC staff's observations of multiple FCF licensees' facilities and cannot be shared publicly, or with the FCF licensees, for security-related and proprietary concerns. The following is a non-sensitive summary of the referenced report:

During the evaluation, the NRC staff observed that the scope of cyber security programs, policies, and procedures at licensee facilities varies greatly across the nuclear fuel cycle industry. The staff also observed that licensees rely on a variety of digital

technologies for the performance of SSEPMCA functions. These range from traditional information technology equipment and software to specialized commercial, proprietary, and hybrid industrial automation systems.

As a result of the NRC staff's observations (see Section 3.3 of this document), the NRC staff recommends a programmatic means for achieving adequate protection against cyber attacks at fuel cycle facilities that (1) provides licensees the flexibility needed to adapt their on-site programs to address emergent cyber threats, and (2) ensures these programs establish and maintain comprehensive cyber security practices for critical digital systems that are used to meet NRC requirements.

2.1.6 Fuel Cycle Cyber Security Working Group – Options for Commission: SECY-14-0147 and the SRM to SECY-14-0147

In SECY-12-0088, the NRC staff stated that it planned to submit a paper seeking Commission approval to initiate a cyber security rulemaking for FCF licensees. In 2011, the working group initiated discussions with the Nuclear Energy Institute (NEI) and FCF licensees on a voluntary industry initiative that would strengthen licensee cyber security. The working group recommended six near-term actions for NEI and FCF licensees to consider in the voluntary industry initiative:

1. establish a cyber security team (CST);
2. provide cyber security awareness training to staff;
3. establish a cyber security incident response capability;
4. provide security controls that address portable media, devices, and equipment (PMDE);
5. perform a baseline assessment of digital assets performing SSEPMCA functions to understand the connections between digital assets and other systems, interactions between digital assets, and interdependencies between digital assets; and
6. provide security controls to isolate digital assets performing critical SSEPMCA functions from external, network-based attack vectors.

SECY 12-0088 stated that if the NRC staff determined that the voluntary actions did not generate the desired outcome of strengthening existing cyber security for FCF licensees, the NRC would consider proposing the issuance of security orders.

On June 14, 2012, the NRC staff convened a classified cyber security threat briefing and progress meeting for licensees to discuss the cyber security threat environment. This classified meeting was followed by an unclassified briefing for licensees on the cyber security threat provided by representatives from the U.S. Department of Homeland Security (DHS), Industrial Control System – Computer Emergency Response Team (ICS–CERT). Additional discussion of the threat and potential vulnerabilities was held on May 30, 2013, during a Threat Workshop for licensees that included sensitive, security-related presentations on advanced persistent threat and security of industrial control systems (ICS), an expert panel discussion, and three technical demonstrations (ADAMS Accession No. ML13168A386).

In several letters submitted to the NRC (not publicly available because they contain security-related information, ADAMS Accession Nos. ML14174B272, ML14174B231, and ML14174B308), NEI agreed that cyber security should be a top priority for FCF licensees and recognized the credibility of potential cyber security threats. NEI indicated that FCF licensees would independently consider the first four near-term voluntary actions the NRC working group recommended (baseline assessment and isolation were excluded). However, FCF licensees clarified during public meetings in the summer and fall of 2014 that they do not plan to:

- incorporate the voluntary actions into an enforceable license amendment,
- establish an implementation schedule or timeframe for implementation of voluntary actions, or
- develop guidance on the implementation of voluntary actions.

Upon further discussions and site visits with FCF licensees, the NRC staff determined that the four voluntary actions proposed by the NEI and FCF licensees only addressed certain safety concerns and did not fully address protection of SSEPMCA functions. The NRC staff's position was that, at a minimum, digital assets performing SSEPMCA functions that, if compromised, could result in a consequence of concern should be protected from a cyber attack. The working group concluded that the six near-term measures proposed would provide assurance of adequate protection to the public health and safety and the common defense and security, while the NRC pursued a cyber security rulemaking for FCF licensees.

In 2014, the working group concluded their effort and the NRC staff issued SECY-14-0147, "Cyber Security for Fuel Cycle Facilities" (not publicly available because it contains security-related information, ADAMS Accession No. ML14177A264). In SECY-14-0147, the NRC staff concluded that cyber security requirements for FCF licensees need to be enhanced because of an increasing and persistent cyber security threat, the potential exploitation of vulnerabilities through attack vectors, the inherent difficulty of detecting the compromise of digital assets, and the potential consequences associated with a cyber attack. SECY-14-0147 provided the following three options for Commission consideration:

1. issuance of a facility-type security order to FCF licensees followed by a rulemaking (NRC staff-recommended option),
2. a rulemaking, or
3. no action.

The NRC staff has concluded that if compromised by a cyber attack, the availability and reliability of SSEPMCA functions required by the regulations, as described in 10 CFR Parts 70, 73, 74, and 95, could be adversely impacted in a manner undetectable until the function fails to perform when needed. The NRC staff's position was that these regulatory required functions must be protected in a manner sufficient to adequately protect public health and safety and the common defense and security. The NRC staff recognized the voluntary actions implemented by industry; however the NRC staff concluded that these actions lacked a comprehensive analysis and, in certain cases, addressed only a limited number of cyber security controls.

In the SRM to SECY-14-0147, the Commission directed the NRC staff to proceed directly with a cyber security rulemaking designated as a high priority and that the final rule should be completed and implemented in an expeditious manner. The Commission also stated that the staff should augment the work performed to date to develop the technical basis for a proposed rulemaking and interact with the stakeholders in developing the proposed and final rule. In developing a more fulsome technical basis, the staff should ensure an adequate, integrated look at cyber security as one aspect of site security (for example, site access controls provide an element of digital asset protection) and take the requisite care to avoid unintended adverse consequences to safety based on a stand-alone focus on cyber security. The technical basis should address the need to integrate the regulatory consideration of safety and security and the necessity to apply a disciplined, graded approach to the identification of digital assets and a graded, consequence-based approach to their protection.

The SRM to SECY-14-0147 also directed the NRC staff to monitor implementation of any voluntary cyber security measures undertaken by FCF licensees. As stated by industry in a public meeting held on June 11, 2015 (ADAMS Accession No. ML15174A130), each facility plans to implement four voluntary actions (establish a CST; provide cyber security awareness training to staff; establish a cyber security incident response capability; and provide security controls that address PMDE) on a site-specific basis. No industry-wide guidance would be issued. The NRC staff conducted site visits at specific facilities during the summer and fall of 2015 to gain an understanding of the implementation of any voluntary actions to better inform the proposed rulemaking effort (ADAMS Accession No. ML15292A098). In general, all licensees were being proactive with their cyber security efforts. The NRC staff observed areas of improvement since the previous site visits several years before and all FCF licensees have plans for further improvement. Overall, the voluntary actions continue to lack comprehensive analysis and, in certain cases, only address a limited number of cyber security controls. In addition, the voluntary actions are not consistently based on a robust risk-management methodology (e.g., NIST SP 800-37, Rev. 1) and have been implemented in a manner that results in an ad hoc approach to the application of cyber security controls. The NRC staff maintains that, based on the developing threat of cyber security attacks and the potential for a consequence of concern, the voluntary actions by FCF licensees lack a level of rigor commensurate with the current cyber security risk environment.

2.1.7 Related Publications

The NRC staff gathered information from various publications while performing their regulatory assessment. Several sources are referenced within the text of this regulatory basis document; however, the following publications were not documented elsewhere but were reviewed as a part of this effort.

Chatham House, the Royal Institute of International Affairs, "Cyber Security at Civil Nuclear Facilities Understanding the Risks," October 2015. Available at: https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf

International Atomic Energy Agency, "Computer Security at Nuclear Facilities," Technical Guidance Reference Manual, Nuclear Security Series No. 17, December 2011.

International Atomic Energy Agency, “NST036 – Computer Security of Instrumentation and Control Systems at Nuclear Facilities,” Draft Guidance Document, November 2014.

International Atomic Energy Agency, “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities,” INFCIRC/225, Revision 5, Nuclear Security Series No. 13, January 2011.

International Atomic Energy Agency, Office of Public Information and Communication, “Secure Computer Systems Essential to Nuclear Security, Conference Finds,” June 8, 2015. Available at: <https://www.iaea.org/newscenter/news/secure-computer-systems-essential-nuclear-security-conference-finds>

U.S. Department of Energy, Office of Inspector General, Audit Report DOE-OIG-16-02, “The Department of Energy’s Cyber Security Risk Management Framework,” November 2015. Available at: <http://energy.gov/sites/prod/files/2015/11/f27/DOE-OIG-16-02.pdf>

U.S. Department of Homeland Security, Recommended Practice, “Improving Industrial Control Systems Cyber Security with Defense-In-Depth Strategies,” October 2009. Available at: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf

2.2 Existing Fuel Cycle Cyber Security Regulatory Framework

2.2.1 NRC Security Orders

The ICM Orders issued to FCF licensees in 2002 and 2003 identified a cyber attack as a credible attack vector; however the ICM Orders contain only one provision that directs licensees to address cyber security vulnerabilities. The associated guidance for the ICM Orders primarily focuses on licensees being able to establish and maintain communications during emergency response actions.

2.2.2 NRC Regulations

Security for FCF licensees is addressed in various sections of the NRC’s regulations. However, as discussed below, many of these sections deal with physical security or information security but do not address cyber security requirements.

10 CFR PART 20, “STANDARDS FOR PROTECTION AGAINST RADIATION”

The regulations in this part establish standards for protection against ionizing radiation resulting from activities conducted under any NRC license. Specific to security, §§ 20.1801 and 20.1802 require licensees to secure from unauthorized removal or access licensed materials that are stored in controlled or unrestricted areas. There are no cyber security requirements for FCF licensees in 10 CFR Part 20.

10 CFR PART 25, "ACCESS AUTHORIZATION"

The regulations in this part establish procedures for granting, reinstating, extending, transferring, and terminating access authorizations of licensee personnel, licensee contractors or agents, and other persons who may require access to classified information. FCF licensees who possess classified material or information are required to comply with 10 CFR Part 25. There are no cyber security requirements for FCF licensees in 10 CFR Part 25.

10 CFR PART 40, "DOMESTIC LICENSING OF SOURCE MATERIAL"

The regulations in this part establish procedures and criteria for the issuance of licenses to receive title to, receive, possess, use, transfer, or deliver source and byproduct materials, as defined in this part, and establish and provide for the terms and conditions upon which the Commission will issue such licenses. These regulations also provide for the disposal of certain byproduct material, as defined in Section 11e.(2) of the Atomic Energy Act of 1954, as amended (AEA), and for the long-term care and custody of byproduct material and residual radioactive material. The regulations in this part also establish certain requirements for the physical protection of import, export, and transient shipments of natural uranium.

Specific to security, FCFs licensed under 10 CFR Part 40 must meet the general requirements in §§ 40.32 and 40.41 that licensed activities must not be inimical to the common defense and security. In addition, § 40.31 requires protection of safeguards information (SGI) against unauthorized disclosure in accordance with the requirements in 10 CFR Part 73 (e.g., 10 CFR 73.21, 73.22, and 73.23), as applicable. There are no cyber security requirements for FCF licensees in 10 CFR Part 40.

10 CFR PART 70, "DOMESTIC LICENSING OF SPECIAL NUCLEAR MATERIAL"

The regulations in this part establish procedures and criteria for the issuance of licenses to receive title to, own, acquire, deliver, receive, possess, use, and transfer SNM; and establish and provide for the terms and conditions upon which the Commission will issue such licenses.

Specific to safety, FCFs licensed under 10 CFR Part 70 must establish and maintain a safety program that demonstrates compliance with the performance requirements of § 70.61. The integrated safety analysis (ISA) is part of the safety program, as required by § 70.62. The ISA must identify certain radiological hazards, chemical hazards, and facility hazards. The ISA is also required to identify potential accident sequences caused by process deviations or other events internal to the facility and credible external events, including natural phenomena. Furthermore, the ISA must identify the consequence and the likelihood of occurrence of each potential accident sequence and the methods used to determine the consequences and likelihoods. The ISA is not required to consider malicious actors, nor is it required to consider any specific cyber security requirements.

Specific to security, FCFs licensed under 10 CFR Part 70 must meet the general requirements in §§ 70.31 and 70.32 that licensed activities must not be inimical to the common defense and security. In addition, § 70.22 contains additional specific requirements for certain types of facilities to have an approved security plan. § 70.22 also requires protection of SGI against unauthorized disclosure in accordance with the requirements in 10 CFR Part 73 (e.g., 10 CFR 73.21, 73.22, and 73.23), as applicable, and must protect classified information in accordance

with the requirements of 10 CFR Parts 25 and 95, as applicable. Furthermore, § 70.22 requires certain licensees establish a program for control and accounting of SNM in the licensee's possession to show how compliance with the requirements of 10 CFR Part 74, as applicable, will be accomplished. There are no cyber security requirements for FCF licensees in 10 CFR Part 70.

10 CFR PART 73, "PHYSICAL PROTECTION OF PLANTS AND MATERIALS"

The regulations in this part establish requirements for the establishment and maintenance of a physical protection system which will have capabilities for the protection of SNM at fixed sites and in transit and of plants in which SNM is used. §§ 73.20, 73.45, and 73.46 contain a general requirement that licensed activities must not be inimical to the common defense and security. Certain FCF licensees are required to comply with applicable requirements in 10 CFR Part 73. The only requirements in § 73.20 require Category I FCF licensees to design their physical protection systems to protect against the DBTs defined in § 73.1. The DBTs, as discussed in Section 2.1.2 of this document, include a cyber attack.

10 CFR PART 74, "MATERIAL CONTROL AND ACCOUNTING OF SPECIAL NUCLEAR MATERIAL"

The regulations in this part establish requirements for the control and accounting of SNM at fixed sites and for documenting the transfer of SNM. General reporting requirements as well as specific requirements for certain licensees possessing SNM of low strategic significance, SNM of moderate strategic significance, and formula quantities of SSNM are included. Requirements for the control and accounting of source material at enrichment facilities are also included.

MC&A and physical protection are part of the NRC's domestic safeguards program. Safeguards are generally understood to be: (1) measures taken to deter, prevent, or respond to the unauthorized possession or use of significant quantities of SNM through theft or diversion; and (2) measures taken to protect against radiological sabotage of nuclear activities. Certain FCF licensees are required to comply with 10 CFR Part 74. § 74.19 addresses the accuracy of records; however there are no cyber security requirements for FCF licensees in 10 CFR Part 74.

10 CFR PART 95, "FACILITY SECURITY CLEARANCE AND SAFEGUARDING OF NATIONAL SECURITY INFORMATION AND RESTRICTED DATA"

The regulations in this part establish requirements for maintaining security clearances and safeguarding Secret and Confidential National Security Information (NSI) and/or Restricted Data (RD). Certain FCF licensees are required to comply with 10 CFR Part 95. § 95.49 requires the approval of the cognizant security agency for automatic data processing systems to utilize or produce classified data or information. However, there are no cyber security requirements for unclassified systems or physical security controls protecting classified information or matter at FCF licensees in 10 CFR Part 95.

2.2.3 NRC Voluntary Reporting Criteria

In September 2013, the NRC issued Information Assessment (IA)-13-02, "Criteria for Reporting Cyber Security Incidents" (not publicly available because it contains security-related information,

ADAMS Accession No. ML13266A214) to FCF licensees. The IA provided additional guidance for voluntary reporting of cyber incidents and cyber security threat information as well as examples of cyber incidents specific to FCF licensees. The IA supplemented several previously issued NRC IAs regarding reporting of suspicious activity, spear phishing activity, and using the NRC Protected Web Server.

2.2.4 Other Federal Laws and Regulations Addressing Cyber Security

Most existing Federal laws governing cyber security are focused on the protection of information and not protection of vital functions (e.g., protecting public health and safety). Federal cyber security statutes and regulations include the 1996 Health Insurance Portability and Accountability Act, the 1999 Gramm-Leach-Bliley Act, the 2002 Homeland Security Act that included the Federal Information Security Management Act (FISMA), the 2013 EO 13636 - Improving Critical Infrastructure Cyber Security, the Cybersecurity Enhancement Act of 2014, the 2014 Cybersecurity Workforce Assessment Act, the National Cybersecurity Protection Act of 2014, and the Cybersecurity Act of 2015.

The 1996 Health Insurance Portability and Accountability Act, the 1999 Gramm-Leach-Bliley Act, and the 2002 Homeland Security Act mandate that specific industries (i.e., healthcare organizations, financial institutions, and Federal agencies) should protect their systems and information. These three statutes do not address protection of systems and information in the private sector, such as FCF licensees, nor do the regulations contain specify cyber security measures that must be implemented.

EO 13636 recognizes that the national and economic security of the nation depends on the reliable functioning of critical infrastructure. EO 13636 directed NIST to work with stakeholders to develop a voluntary framework—based on existing standards, guidelines, and practices—for reducing cyber risks to critical infrastructure. The Cyber Security Enhancement Act of 2014 reinforced NIST's EO 13636 role. Given the voluntary nature of the NIST framework, the statute does not contain specify cyber security measures that must be implemented by FCF licensees.

The 2014 Cybersecurity Workforce Assessment Act directed DHS to conduct a triennial assessment of the DHS cybersecurity workforce. The National Cybersecurity Protection Act of 2014 codified an existing operations center for cybersecurity. These two statutes do not address protection of systems and information in the private sector, such as FCF licensees, nor do the regulations contain specify cyber security measures that must be implemented.

Most recently, the Cybersecurity Act of 2015 requires federal entities that regulate critical infrastructure, to: (1) assess entities identified under EO 13636, which provides for the identification of critical infrastructure where a cyber security incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security; (2) report to Congress regarding the extent to which such entities report significant intrusions of information systems essential to the operation of critical infrastructure to DHS or appropriate agency heads in a timely manner; and (3) develop a strategy to ensure that a cyber security incident affecting such entities would no longer reasonably result in such catastrophic regional or national effects. This statute only applies to critical infrastructure and does not contain specify cyber security measures that must be implemented.

2.2.5 Other Federal Agencies Involved in Cyber Security

DHS:

DHS ICS-CERT is a key component of the national Strategy for Securing Control Systems. The primary goal of the Strategy for Securing Control Systems is to build a long-term, common vision where effective risk management of control systems security can be realized through successful coordination efforts. DHS ICS-CERT leads this effort by: responding to and analyzing control systems-related incidents; conducting vulnerability, malware, and digital media analysis; providing onsite incident response services; providing situational awareness in the form of actionable intelligence; coordinating the responsible disclosure of vulnerabilities and associated mitigations; and sharing and coordinating vulnerability information and threat analysis through information products and alerts. In addition, DHS ICS-CERT coordinates control systems related security incidents and information sharing with Federal, State, Tribal, Territorial, and local agencies and organizations, the intelligence community, and private sector constituents, including vendors, owners, and operators. DHS ICS-CERT provides a direct path for coordination of activities among all members of the critical infrastructure stakeholder community.

NIST:

In February 2014, in response to EO 13636, NIST released the Framework for Improving Critical Infrastructure Cyber Security (Framework). The Framework uses a common language to address and manage cyber security risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses. The Framework focuses on using business drivers to guide cyber security activities and considering cyber security risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cyber security activities, outcomes, and informative references that are common across critical infrastructure sectors and provides the detailed guidance for developing an individual organizational Profile. Through use of this Profile, the Framework assists an organization to align its cyber security activities with its business requirements, risk tolerances, and resources. The Implementation Tiers provide a mechanism for an organization to view and understand the characteristics of their approach to managing cyber security risk.

DOE:

The DOE Cyber Security Program (CSP) establishes requirements and responsibilities for a cyber security program to protect information and information systems for DOE. The DOE CSP requires a risk management approach that includes: analysis of threats/risks; risk-based decisions considering security, cost and mission effectiveness; and implementation consistent with NIST guidelines and the Committee on National Security Systems cyber requirements, processes, and protections. DOE oversight is conducted through assurance systems that monitor the risk evaluation and protection processes at each level in the organization. The DOE CSP emphasizes risk management rather than a systems-level "controls compliance" approach.

2.3 NRC Authority for Rulemaking

Section 161.b of the AEA gives the Commission the authority to "establish by rule, regulation, or order, such standards and instructions to govern the possession and use of special nuclear

material, source material, and byproduct material as the Commission may deem necessary or desirable to promote the common defense and security or to protect health or to minimize danger to life or property.” Consistent with this authority, the Commission can authorize the staff to engage in a rulemaking to develop cyber security requirements applicable to FCF licensees.

2.4 Summary

The NRC currently has no cyber security regulations codified in 10 CFR for FCF licensees. The current regulatory framework to address cyber security for FCF licensees is based on a single provision in the ICM orders that instructs licensees to address cyber security vulnerabilities. Additionally, the DBT was revised in 2007 to explicitly include cyber attacks. The ICM Orders, the DBT, and the associated guidance for the orders and the DBT do not establish specific security requirements for protecting against cyber attacks or establishing a formal cyber security program.

FCF licensees have implemented a number of cyber security controls in recognition of the potential threats from a cyber attack for both business and safety considerations. However, implementation of these controls is highly variable and lacks appropriate rigor and documentation. Therefore, the NRC staff, in compliance with the Commission’s direction in the SRM to SECY-14-0147, plans to conduct a high priority cyber security rulemaking for FCF licensees that would provide for the completion and implementation of the final rule in an expeditious manner. The staff plans to adopt a graded, risk-informed, performance-based approach for the proposed rulemaking to develop appropriate cyber security requirements for FCF licensees.

Chapter 3 Regulatory Problem

This chapter explains the need for new cyber security requirements for FCF licensee activities involving source material, SNM, and hazardous chemicals regulated by the NRC. The discussion addresses the following issues:

- cyber security threats and attack vectors;
- vulnerabilities and pathways;
- lack of a robust and comprehensive regulatory framework; and
- potential consequences.

3.1 Cyber Security Threats and Attack Vectors

Cyber security threats refer to individuals or entities who attempt unauthorized access to a digital asset, system, or network. This access can be directed by trusted users (either intentionally or unintentionally) or by unknown actors, and originate from within an organization or from remote locations using the Internet. Threats to digital assets, systems, or networks can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, careless system users, and bored or curious individuals.

An attack vector is a pathway or tool used to gain access to a digital asset, system, or network in order to launch attacks, gather information, deny services, or deliver/leave a malicious item or items in those devices, systems, or networks. The number and sophistication of attack vectors tends to grow as advancements in technology provide additional pathways. The popularity of mobile computing offers more pathways and tools that can be used to launch attacks, gather information, or deliver/leave malicious applications. Some common attack vectors include the following:

- Phishing attacks can use a network's applications and systems against its own users. For example, a company-wide e-mail may include maliciously crafted links to viruses or malware. Additionally, detailed information regarding a network's users can be gathered on the Internet via public archives and social networking sites. This information can be used to conduct targeted phishing attacks (i.e., spearfishing) against individual users that can be very difficult to detect.
- Unsecured or inadequately secured wireless networks can be used as both a tool and a pathway for launching certain cyber attacks. If attackers are able to gain unauthorized access to a wireless network, they can observe traffic, insert or exfiltrate data, launch attacks, and deny services to legitimate users.
- Removable and portable media, such as universal serial bus (USB) drives, can easily introduce malware into an information system, even if the system is air-gapped (i.e., physically isolated from and unconnected to an unsecured network). The threat does not need to be actively involved if an unsuspecting individual (e.g., employee) connects a compromised USB drive to the organization's computer system or network.

- Mobile devices (e.g., smartphones and tablets) can be used both as a tool and a pathway for launching attacks or gathering personal information. Insufficient configuration management controls allow mobile devices to introduce potential vulnerabilities.
- Embedded code can be used as a tool to launch attacks using malicious Web pages. Attacks in the form of malicious downloads may occur as a result of unsuspecting individuals visiting Web pages that contain malicious components.
- Viruses and malware are tools that are used to launch certain types of attacks. Many of these tools are openly available on the Internet. Such attacks will have differing goals based on the threat actor, environment, and target system or network.
- The supply chain for equipment containing digital assets (e.g., manufacturers, vendors, service providers) can allow threats to introduce vulnerabilities when digital assets are acquired, updated, or maintained, such as the introduction of compromised tools during vendor maintenance activities.

The attack vectors listed above (and others not listed) can be used individually, or in conjunction, to launch cyber attacks. As cyber security threats become more sophisticated and attack methods multiply, the list of attack vectors will continue to grow.

Cyber attacks can be initiated by a range of actors including nation states, individuals, or insiders. The attacks can be implemented remotely, over a broad timeframe, and impact multiple systems with an immediate or delayed compromise to 3S functions. Because of these characteristics, the potential for a cyber attack to be implemented, penetrate boundaries, remain undetected, and compromise 3S functions performed by digital assets is significantly higher for a cyber attack than for a physical attack.

FCF licensees are becoming increasingly reliant on digital technologies to enhance and maintain plant productivity and perform safety, security, and safeguards (3S) functions. Examples of specific 3S functions are provided in Section 4.4 of this document.²

The NRC staff has observed that some 3S functions are extensively controlled by digital assets. Additionally, many of these 3S functions are commingled with business and plant networks and either directly or indirectly connected to the Internet. This increases their accessibility and susceptibility to cyber attacks. In order to adequately protect 3S functions, it is essential that FCF licensees understand and take measures to protect against cyber security threats and attack vectors.

² As explained further in Section 4.4, the NRC staff has refined its position with regard to the functions performed by digital assets within the scope of the proposed rulemaking. The current NRC staff position is that licensees should, at a minimum, protect from a cyber attack those digital assets that perform 3S functions (rather than all SSEPMCA functions) and whose compromise could result in a consequence of concern.

Large industrial facilities, including at least one FCF, have fallen victim to cyber attacks. The following are known cyber attacks:

The Stuxnet worm, which targeted Iran's Natanz FCF, successfully infected an ICS isolated by an air gap. The Stuxnet worm covertly monitored and compromised safety systems and surreptitiously manipulated system settings to cause gas centrifuges to fail/crash, adversely impacting the uranium enrichment process. The Stuxnet worm was designed to target a specific brand and version of ICS similar to what is used at FCF licensees in the United States. An attack on an FCF licensee's ICS could adversely impact systems and processes relied on by the licensee to protect public health and safety and common defense and security. This attack originated as a sophisticated malware program, but is now in the public domain for others to manipulate and use for their own purposes.

The Shamoon virus, which targeted the Saudi Aramco oil facility, successfully infected 30,000 computers, exported company information to the attacker(s), and then damaged the computers by overwriting the master boot record making the computers unbootable. This attack originated as a sophisticated malware program, but is now in the public domain for others to manipulate and use for their own purposes.

The BlackEnergy malware, whose target appears non-specific, has compromised numerous ICS. Analysis by DHS ICS-CERT indicates that this campaign has been ongoing since at least 2011. Multiple companies have identified the malware on internet connected human-machine interfaces (e.g., GE Cimplicity, Advantech/Broadwin WebAccess, and Siemens WinCC). DHS ICS-CERT strongly encourages taking immediate defensive action to secure ICS using defense-in-depth principles. Additional details are listed in the original DHS ICS-CERT Alert released on December 10, 2014 (ICS-ALERT-14-281-01B). The BlackEnergy malware has the potential for unauthorized disclosure of information, unauthorized modification of the ICS, and disruption of service.

The Havex malware, whose target appears non-specific, is associated with an ICS focused malware campaign that uses multiple vectors for infection. These include phishing e-mails, redirects to compromised Websites, and most recently, trojanized update installers on at least three ICS vendor Web sites, in what are referred to as watering hole-style attacks. Additional details are listed in the original DHS ICS-CERT Alert released on June 27, 2014 (ICS-ALERT-14-176-02A). The Havex malware has caused multiple platforms to intermittently crash, which could cause a denial of service effect on applications reliant on certain communications.

The 2014 cyber attack on a steel mill in Germany can be categorized as an advanced persistent threat (attackers gain persistent access to the victim network and then widen the attack to additional systems). In the steel mill attack, the attackers used spear phishing e-mails in tandem with sophisticated social engineering to gain initial access to the steel mill's office network. From there they worked their way progressively into the production networks. The impacts of the attack were breakdowns of individual control components or entire ICS networks. The breakdowns led to the uncontrolled shutdown of a blast furnace, leaving it in an undefined state and resulting in massive damage.

3.2 Vulnerabilities and Pathways

Cyber attacks can only occur when:

1. a vulnerability/weakness exists;
2. a method/means (an exploit) is used to take advantage of the vulnerability; and
3. a pathway/mechanism for delivering the exploit exists.

Without all three of these elements a successful cyber attack is not possible. Often, a given vulnerability can be attacked (and an exploit delivered) via multiple pathways and by multiple means. For example, a weak password can be attacked from across a network via a telnet or secure shell connection or by using malware delivered from portable media. There are also multiple ways of gaining access to a pathway, such as through the supply chain or through social engineering. Access to one pathway may allow access to others. For example, physical access to a digital asset might allow use of a USB port as an added attack pathway unless steps have been taken to prevent such actions.

Successful cyber attacks require the discovery of weaknesses or vulnerabilities that can be exploited in a system or network's cyber security controls. These weaknesses can be technical or process-based (i.e., firewall settings, inadequate procedures). Cyber security threats continue to use various attack vectors (e.g., the Internet, supply chain, portable media, social engineering) to exploit weaknesses and vulnerabilities. The Stuxnet worm demonstrated the successful use of manual delivery via portable devices and media as a pathway for an attack. Even organizations that have good security policies and procedures may be susceptible to malware on infected portable electronic devices brought into their facilities and allowed onto their networks and systems by trusted external partners and suppliers.

The implementation of digital technologies without an understanding of the cyber security threat environment, without the appropriate cyber security analysis, and without the application of sufficient cyber security controls, is likely to result in exploitable weaknesses or vulnerabilities in a site's cyber security. These weaknesses and vulnerabilities may include the following examples:

- implementation of wireless technologies to enable use of portable electronics and smart devices (e.g., smart transmitters) to facilitate point-to-point communication without adequate wireless security mechanisms;
- remotely accessible process automation networks or equipment onto the plant/corporate business network without effective boundary controls and other cyber security protection mechanisms;
- lack of appropriate physical security or controlled access to plant systems and networks, including allowing uncleared/unsupervised vendor personnel to perform maintenance;
- remote connectivity to critical systems by vendor support personnel using dial-up telephone, wireless/cellular, or Internet connectivity;

- allowing factory default settings and passwords to remain in systems/devices; or
- replacement of analog technology with functionally equivalent digital technology with no recognition or analysis of the new vulnerabilities or pathways introduced by the upgrade.

Vulnerabilities in operating systems, networks, and software are continuously being discovered and exploited. Although most researchers, security firms, and vendors generally announce vulnerabilities as they are identified and provide a security patch, there is often a time lag between when security patches become available and when they are implemented in the operational environment. This is especially true for industrial automation systems. In addition, there is a large and robust underground economy based on the buying and selling of exploits of unpatched vulnerabilities. This economy is used by criminals, malcontents, terrorists, and other malicious parties to purchase tools for cyber attacks. Many exploits traded within this economy are for vulnerabilities not yet announced to the general public – they may not even be well-known to the vendor themselves.

3.3 Lack of Robust and Comprehensive Regulatory Framework

The NRC's FCF cyber security working group, established in 2010, reviewed cyber security measures currently in place at FCF licensees to determine how these facilities protect their digital assets from cyber attacks. The working group used an older version of the NIST SP 800-53 guidance document to assist in evaluating the cyber security provided by FCF licensees. NIST SP 800-53 is generally accepted in the cyber security industry and is used extensively at critical infrastructure facilities. In conducting this review, the working group specifically looked at digital assets performing, supporting, or associated with critical functions, such as SSEPMCA, that if compromised, could impact public health and safety or common defense and security. The assessment included the following:

1. requesting FCF licensees to respond to an NRC questionnaire regarding the extent to which digital assets were used to perform SSEPMCA functions;
2. performing site visits to a representative cross section of the FCF licensees; and
3. analyzing licensees' documentation of their cyber security programs and observing how the programs were implemented.

Some general areas of concern identified by the working group during the assessment included, but were not limited to, the following:

- Some process control networks (PCNs), where digital assets that perform SSEPMCA functions were not protected consistent with cyber security controls generally applied to corporate networks.
- Some PCNs, where digital assets perform SSEPMCA functions, were not supported and maintained consistent with the corporate networks.
- There appeared to be an overreliance on physical security programs (e.g., access control) to protect connections to the PCNs.

- Periodic cyber security reviews were not consistently tied to system updates or the performance of maintenance.
- There appeared to be limited capabilities to detect cyber attacks.
- The voluntary actions taken by certain FCF licensees provided limited cyber security controls on portable media and mobile devices.
- The voluntary actions taken by certain FCF licensees provided limited cyber security controls on the use of wireless technologies.
- Network architecture documents did not appear to accurately illustrate system connections between digital assets and dependencies between digital assets.
- The voluntary actions taken by certain FCF licensees provided limited cyber security controls for offsite connections.

Currently, NRC regulations do not specifically address cyber security for FCF licensees. For the majority of FCF licensees, the only NRC cyber security directed requirement comes from the ICM Orders issued in 2002–2003. The ICM Orders contain a single provision that instructs licensees to address cyber security vulnerabilities. The ICM Orders did not direct the establishment of a formal cyber security program nor did they provide a methodology for the identification and protection of digital assets associated with potential consequences of concern. Therefore, the ICM Orders do not create an adequate regulatory framework necessary for effective implementation, oversight, and enforcement of a cyber security program at FCF licensees which may constitute an unreasonable risk to public health and safety. In addition, although the ICM Orders differ for the various types of FCF licensees (i.e., Category I and III FCFs licensed under 10 CFR Part 70 and uranium hexafluoride conversion and deconversion facilities licensed under 10 CFR Part 40), the cyber security requirement focused on licensees being able to maintain offsite communications for EP functions.

Category I FCF licensees are subject to two DBTs (radiological sabotage and theft or diversion of formula quantities of SSNM).³ In accordance with 10 CFR 73.20, Category I FCF licensees must maintain a physical protection system designed to protect against these DBTs. Both DBTs include a cyber attack as a method of attack by adversaries. However, current NRC physical protection requirements do not set forth specific requirements for addressing cyber attacks on Category I FCF licensees.

Under 10 CFR 70.62, certain FCF licensees are required to establish and maintain a safety program that demonstrates compliance with 10 CFR 70.61. One element of the safety program is to conduct and maintain an ISA. The ISA requires licensees to identify hazards (e.g., chemical, radiological), potential accident sequences, and the consequences and likelihood of potential accident sequences, as well as each item relied on for safety (IROFS) identified under 10 CFR 70.61. Licensees are required to implement IROFS to mitigate or prevent accident consequences that have the potential to exceed exposure thresholds, both radiological and

³ FCF licensees, other than Category I facilities, are not subject to a DBT.

chemical, for workers and the public at both high and intermediate levels. NRC's regulations do not require FCF licensees to consider malicious acts, such as cyber attacks, when conducting and maintaining their ISA.

The safety program established and maintained under 10 CFR 70.62 ensures that each IROFS is available and reliable to perform its intended function when needed and meets the performance requirements of 10 CFR 70.61. During site visits at certain FCF licensees, 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 during an event (i.e., may result in a safety consequence of concern).

The cyber security requirements in 10 CFR 73.54 and associated guidance in RG 5.71 were developed for power reactors. The cyber security requirements for power reactors were placed into a stand-alone section of 10 CFR Part 73 to enable these requirements to be made applicable to other types of facilities through future rulemakings. FCF licensees (Category I, II, III, and 10 CFR Part 40) represent a broad spectrum of facility types, processes, and potential consequences that differ from power reactors. The differences in potential consequences among the types of FCF licensees illustrate the need for more flexible cyber security requirements for FCF licensees. As a result, the existing rule in 10 CFR 73.54 is not appropriate to address the unique programs and associated risks specific to FCF licensees.

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

Additional analysis of MC&A programs at FCF licensees should also be considered for the potential electronic alteration of MC&A records. For example, potential electronic alterations may include modification of the category, location, or amount of SNM in FCF licensee records. The NRC staff plans to consider this potential impact to 3S functions during rulemaking.

Digital assets associated with physical security of classified information at FCF licensees are also subject to a risk of cyber attack. Certain FCF licensees (i.e., Category I and Category III

enrichment) are subject to the physical security requirements of 10 CFR Part 95 and must maintain a facility security clearance because they process and store NSI and/or RD. The classified systems and networks that process and store this information have cyber security controls in accordance with DOE or DOD requirements. To avoid dual regulation, the NRC staff expects that the rulemaking would specifically exclude these classified systems, and potentially some unclassified systems, if the digital assets are provided with a level of protection equivalent to the NRC rule and are accredited by another federal government entity. However, the digital assets (e.g., door alarms) associated with the physical security of these classified systems and information fall within the regulatory purview of the NRC as the cognizant security agency for these facilities. Currently, there are no NRC cyber security requirements in place to protect these types of digital assets from cyber attacks. If not adequately protected, these physical security digital assets have the potential to be compromised by a cyber attack and may not be available or reliable during an event (i.e., may result in a security consequence of concern).

As previously discussed in Chapter 2 of this document, some FCF licensees are implementing voluntary actions (e.g., forming a CST, cyber security awareness training, controlling portable media, and establishing an incident response capability) to address cyber security concerns. The voluntary actions implemented by industry lack a comprehensive analysis and, in certain cases, only address a limited number of cyber security controls. The voluntary actions are not consistently based on a robust risk-management methodology (e.g., NIST SP 800-37, Rev. 1) and have been implemented in a manner that results in an ad hoc approach to the application of cyber security controls. The NRC staff has determined that, based on the developing threat of cyber security attacks and the potential for a consequence of concern, the voluntary actions lack a level of rigor commensurate with the developing cyber security risk.

In addition, the voluntary actions do not provide an adequate substitute for a regulatory framework that would facilitate the development of a formal cyber security program. These voluntary actions are not incorporated into each license as a license condition and therefore are not subject to NRC oversight, inspection, or enforcement activities. Furthermore, no industry guidance has been developed, which could lead to inconsistent implementation of voluntary actions. Finally, no timeframe has been established for FCF licensees to implement the four voluntary actions and, as previously stated, a credible cyber security threat exists and continues to evolve and target systems similar to those at FCF licensees.

The NRC provided criteria in IA-13-02 (not publicly available because it contains security-related information, ADAMS Accession No. ML13266A214) for the voluntary reporting of cyber security incidents by FCF licensees. However, these criteria do not have timelines associated with them. Prompt notification of certain cyber security incidents, even though their significance may seem minor, is a safety and security enhancement because it increases awareness of cyber security threats and allows the NRC to notify other licensees and plan for an appropriate response if an attack is substantiated. Additionally, required notification of certain cyber security incidents would assist the NRC in meeting its strategic communications mission of informing the DHS and Federal intelligence and law enforcement agencies of cyber security events that could: (1) endanger public health and safety or the common defense and security, (2) provide information for threat-assessment processes, or (3) generate public or media inquiries.

The existing regulatory framework lacks requirements to address several key aspects of cyber security for FCF licensees. The NRC staff proposes to address the following through a rulemaking:

- formation of a CST,
- training staff on cyber security,
- identification of digital assets associated with a potential consequence of concern;
- application of cyber security controls to digital assets,
- configuration management of digital assets,
- cyber security incident response capability, and
- cyber security event reporting and recordkeeping.

These cyber security aspects are further discussed in Section 4.4 of this document.

3.4 Potential Consequences

The scope and magnitude of the potential consequences from a successful cyber attack vary in degree among FCF licensees. Since FCF licensees include a broad spectrum of facility types and processes, there are a wide variety of potential vulnerabilities and consequences. SNM and hazardous chemicals used by FCF licensees present various safety (e.g., criticality, release of chemicals resulting in significant exposures to workers or members of the public) and security concerns (e.g., theft, diversion of SNM) that could be triggered by a cyber attack if digital assets associated with 3S functions are not adequately protected from cyber attacks.

In 2013, the NRC cyber security working group conducted assessments for certain FCF licensees using a consequence-based approach to review the licensees' SSEPMCA programs. The working group also reviewed the NRC regulations and security orders that govern these programs. The goal of this review was to identify and assess whether, and to what extent, licensees use digital assets to perform SSEPMCA functions and to evaluate the levels of cyber security currently provided to digital assets performing SSEPMCA functions. The results of this review were used to evaluate potential consequences triggered by cyber attacks on FCF licensees.

When considering potential consequences, the facility type plays an important role in identifying digital assets and the recommended protections against cyber attacks. For example, FCF licensees with a DBT would need to identify and protect security functions associated with meeting the requirements of the DBT because of the consequences associated with the potential theft or diversion of SSNM as well as the significant consequences associated with radiological sabotage.

Using the consequence-based approach, the working group determined that FCF licensees do use digital assets to perform SSEPMCA functions, and in many cases, the digital assets associated with SSEPMCA functions may require additional protection from cyber attacks. The following sections provide a summary of each category of SSEPMCA functions reviewed by the working group, and explains how a cyber attack on digital assets associated with these functions could lead to a potential consequence of concern.

As reflected in SECY-14-0147, the NRC staff's position was that, at a minimum, digital assets performing SSEPMCA functions that, if compromised, could result in a consequence of concern should be protected from a cyber attack. The current NRC staff position is that, at a minimum, digital assets performing 3S functions that, if compromised, could result in a consequence of concern should be protected from a cyber attack. The current NRC staff position is reflected in the following subsections discussing 3S functions and the associated consequences of concern.

Note that the term "failure" has a different meaning than the term "compromise." Failure means that the intended function is not performed. Compromise means that an alternate, undesired function occurs which may include failure of the intended function. For example, failure of a wireless signal typically means that the signal is lost. Compromise of a wireless signal means that the signal is being used to perform unintended functions that may be of a malicious nature. Many safety and security analyses previously conducted by FCF licensees consider only failure mechanisms. Conversely, most safety and security analysis do not consider the effects of malicious compromise. It is expected that existing safety and security analyses would help inform the selection of digital assets and reduce the regulatory burden, however some additional considerations may be necessary.

3.4.1 Safety

As previously discussed in Section 3.3 of this document, 10 CFR 70.62 requires certain FCF licensees to establish and maintain a safety program that demonstrates compliance with 10 CFR 70.61. In addition, the safety program established and maintained under 10 CFR 70.62 ensures that each IROFS is available and reliable to perform its intended function when needed and to meet the performance requirements of 10 CFR 70.61. Among 10 CFR Part 40 licensees, a licensee identifies plant features and procedures (PFAPs) that provide a similar functionality as IROFS for 10 CFR Part 70 licensees. PFAPs are intended to remain available and reliable and perform their intended safety functions (i.e., protecting public health and safety) in the event of an accident sequence. FCF licensees establish and maintain IROFS or PFAPs in order to mitigate accident sequences that could result in nuclear criticalities or releases of radioactive materials or chemicals resulting in significant exposures to workers or members of the public.

During the 2013 assessments, the working group determined that FCF licensees use digital assets as IROFS or PFAPs and those digital assets may require additional protection from cyber attacks to limit the risk of a consequence of concern. If the compromise of one of those digital assets were to go undetected and unresolved, the digital asset could fail to perform the intended safety function when needed during an ISA analyzed accident sequence. This type of compromise is being recognized as a latent failure. A latent failure could, in turn, result in a safety consequence of concern (i.e., nuclear criticality or chemical/radiological release resulting in significant exposures to workers or members of the public).

In addition, digital assets associated with operational and process safety functions may be identified that, if compromised by a malicious act, could immediately cause a safety consequence of concern. This type of compromise is being recognized as an active failure. Further evaluation of this topic is expected during rulemaking.

3.4.2 Security

The working group determined that FCF licensees use digital assets to perform security functions associated with meeting the requirements of certain facility-type security orders (e.g., revised DBT, ICM), 10 CFR Part 73 requirements, site-specific security plan commitments, and 10 CFR Part 95 requirements associated with the protection of classified NSI and RD. In addition, Category I FCF licensees utilize digital assets in order to provide high assurance that activities involving SNM are not inimical to the common defense and security, meet DBT requirements, and do not constitute an unreasonable risk to the public health and safety.

During the 2013 assessments, the working group determined that the digital assets being used by FCF licensees to perform certain security functions may require additional protection from cyber attacks to limit the risk of a consequence of concern. If a compromise of one of these digital assets due to cyber attack were to go undetected and unresolved, the digital asset could fail to perform its intended security function (e.g., deter, detect, assess, delay, respond, communicate) when needed to maintain the facility's physical protection system. This failure could, in turn, result in a security consequence of concern (i.e., theft or diversion of SNM, radiological sabotage, loss or unauthorized disclosure of classified material).

3.4.3 Emergency Preparedness

In accordance with applicable regulations (10 CFR 40.31 and 70.22), FCF licensees are required to establish, maintain, and follow an emergency plan. FCF emergency plans provide the capability to respond to different types of alarms in a timely manner, mitigate consequences of accidents, assess releases of radioactive materials, and conduct timely notifications (e.g., protective action recommendations) in the event of an accident or emergency.

During the 2013 assessments, the working group determined that the digital assets used by FCF licensees to perform EP functions may require additional protection from cyber attacks to limit the risk of a consequence of concern. If a compromise of one of these digital assets due to cyber attack were to go undetected and unresolved, the digital asset could fail to perform its intended EP function (e.g., detect alarms, assess radioactive release, conduct timely notifications) when needed during an emergency.

Based on follow-up site visits in 2015, the working group recognizes that diversity of functions and capabilities exists such that non-digital redundancies are present for most EP functions. Therefore, it is unlikely that a compromise of a digital asset could prevent the licensee from accomplishing the intended function (i.e., maintain onsite and offsite communications during normal and emergency operations). The NRC staff expects that the rulemaking would require protection of EP functions only in cases where they support (i.e., provide an input to) 3S functions associated with a consequence of concern.

3.4.4 MC&A

Consistent with 10 CFR Part 74, certain FCF licensees are required to implement and maintain an NRC-approved MC&A system. The MC&A system must achieve certain general performance objectives based on the quantity of SNM possessed (i.e., Category I, II, or III quantities). The greater the quantity of SNM possessed, the greater the potential consequences of concern (e.g., loss, theft, or diversion of SNM). Licensees utilize MC&A functions for inventory reconciliation and to meet international treaty requirements.

During the 2013 assessments, the working group determined that the digital assets used by FCF licensees to perform MC&A functions may require additional protection from cyber attacks to limit the risk of a consequence of concern. If a compromise of one of these digital assets due to cyber attack were to go undetected and unresolved, the digital asset could fail to perform its intended MC&A function (e.g., identify, resolve indications of missing material).

For purposes of the proposed rulemaking, the MC&A function is now considered a safeguards function that can have varying degrees of risk based on facility-type (e.g., Category I, II, or III). The NRC staff expects that the rulemaking would require protection of certain safeguards functions if associated with a consequence of concern.

In addition, some of the safeguards functions are integrated with IROFS, so a compromise of a safeguards function could cause a compromise of one or more safety functions as well. This compromise could, in turn, result in a safety consequence of concern (i.e., significant exposure events such as criticality). The NRC staff expects that the rulemaking would require protection of certain safeguards functions in cases where they support (i.e., provide an input to) 3S functions associated with a consequence of concern.

3.5 Summary

Potential attack vectors are expected to grow as cyber security threats become more sophisticated and attack methods multiply. Globally, vulnerabilities in existing operating systems, networks, and software are continuously being discovered and exploited. In order to adequately protect 3S functions, it is essential that FCF licensees understand and take measures to protect against cyber security threats and attack vectors.

Currently, there are no NRC regulations governing cyber security for FCF licensees. The NRC assessments of several FCF licensees identified digital assets that perform 3S functions which may require additional protection. If the compromise of one of those digital assets were to go undetected and unresolved, the cyber attack could:

- directly result in a safety consequence of concern (i.e., active); or
- compromise a function needed to prevent, mitigate, or respond to a 3S event associated with a consequence of concern (i.e., latent).

The NRC staff has determined that, based on the developing threat of cyber security attacks, the voluntary actions taken by FCF licensees lack a level of rigor commensurate with the developing cyber security risk. Furthermore, the voluntary actions do not provide an adequate substitute for a regulatory framework requiring development of a formal cyber security program.

Chapter 4 Basis for Requested Change

This chapter explains the proposed changes to NRC regulations and discusses the technical rationale and assumptions used to support those changes. This chapter also discusses how the proposed changes can resolve the issues identified in Chapter 3 of this document. At a high level, the rulemaking would consider changes to the regulations that: (1) utilize a graded, consequence-based approach for the identification and protection of digital assets associated with 3S functions at FCF licensees, (2) utilize the operational experiences gained from the development and implementation of 10 CFR 73.54, and (3) build upon cyber security requirements and commitments implemented through security orders and voluntary actions. The rulemaking seeks to create a comprehensive regulatory framework that establishes and maintains a flexible cyber security program that can adapt to the constantly evolving cyber security threat.

4.1 Commission Direction

On March 24, 2015, the Commission issued the SRM to SECY-14-0147, which approved immediate initiation of a high priority cyber security rulemaking for FCF licensees and stated that the final rule should be completed and implemented in an expeditious manner. In addition, the SRM to SECY-14-0147 directed that the staff augment the work performed to date to develop a more fulsome technical basis and interact with stakeholders in developing the proposed and final rule. The Commission also requested that the technical basis address the need to integrate the regulatory consideration of safety and security and the necessity to apply a disciplined, graded approach to the identification of digital assets and a graded, consequence-based approach to their protection.

4.2 Proposed Changes

The NRC staff envisions a rulemaking that addresses the current cyber security threat environment through a comprehensive regulatory framework that addresses cyber security for FCF licensees. As previously discussed in Chapter 3 of this document, the NRC has issued orders and modified the DBT to require FCF licensees to protect against cyber attacks. However, the NRC has not developed a regulatory framework or specific regulations that address cyber security for FCF licensees. The ICM Orders did not establish a regulatory framework for the consistent application of cyber security for FCF licensees. Currently, each FCF is addressing cyber security independently and on their own timeline. Assessments conducted from 2011 through 2013 led the staff to determine that adequate cyber security for FCF licensees requires a comprehensive regulatory framework that incorporates a graded, consequence-based approach that can be consistently implemented for the long-term protection of public health and safety and promotion of common defense and security.

Based on the discussion in Chapter 3 of this document (e.g., increasing and persistent cyber security threat, the vulnerabilities identified in existing attack vectors, the inherent difficulty of detecting the compromise of a digital asset, the lack of voluntary actions with a level of rigor commensurate with the developing cyber security risk, and the potential consequences associated with a cyber attack), the NRC staff concludes that there is a need to establish and maintain consistent cyber security requirements for the protection of FCF licensees. In the areas of safety, security, and safeguards, a cyber attack can compromise the availability and reliability of certain 3S functions which could go undetected until the function fails to perform

when needed, which could result in a consequence of concern. The NRC staff's position is that these critical 3S functions must be protected in a manner sufficient to adequately protect public health and safety and promote the common defense and security.

Therefore, the NRC staff is considering a rulemaking that would develop applicable rule language informed by the existing language in 10 CFR 73.54. The NRC staff recognizes that FCF licensees have operational characteristics and potential consequences that differ from those of power reactors. Accordingly, the proposed rulemaking would be tailored to provide an adequate level of protection from a cyber attack, given the specific operational characteristics and potential consequences at FCF licensees. The proposed rulemaking would take into account differences in the various types of FCF licensees by implementing a facility-type graded approach, establish thresholds for consequences of concern, and develop methodologies for the identification (screening) and protection (application of controls) of digital assets.

The NRC staff's initial approach is to propose a new section for 10 CFR Part 73. This new language would require FCF licensees to implement a formalized cyber security program that is flexible and able to evolve in tandem with emergent cyber security threats; limits the spread of cyber attacks across digital assets; minimizes the potential consequences from cyber attacks; and aids in the identification and recovery from a cyber attack. The staff also plans to develop rule language that ensures cyber security requirements would not obstruct a licensee's ability to meet other regulatory requirements. The anticipated rule language must also provide the Commission with assurance that the public health and safety and the common defense and security are adequately protected. Furthermore, the staff plans to develop rule language to permit various approaches based on facility type, similar to those anticipated in the associated guidance document (e.g., risk-management framework from NIST SP 800-37, Rev. 1; screening methodology for digital assets to account for equivalent 3S function provided by alternate means; graded technique to risk-inform application of cyber security controls; and evaluation considerations from NIST SP 800-53, Rev. 4, for specific cyber security controls).

4.3 Technical Approach

FCF licensees (conversion, enrichment, power reactor fuel fabrication, and naval nuclear fuel fabrication) each have varying potential consequences of concern related to safety, security, and safeguards. To account for these differences, the NRC staff plans to develop a rulemaking approach that takes into account facility type and would apply a risk-informed, performance-based, and graded approach for the protection of digital assets from a cyber attack.

A consequence-based approach to identifying digital assets that takes into account the type of facility would be considered in the development of a comprehensive regulatory framework to address cyber security for FCF licensees. It is expected that this regulatory framework would protect digital assets associated with 3S functions from cyber attacks that could:

- directly result in a safety consequence of concern (i.e., active); or
- compromise a function needed to prevent, mitigate, or respond to a 3S event associated with a consequence of concern (i.e., latent).

The consequences of concern under consideration are:

- significant exposure events that could endanger the life of workers or could lead to irreversible or other serious, long-lasting health effects to workers or members of the public (e.g., nuclear criticalities and releases of radioactive materials or chemicals) [safety];
- radiological sabotage and theft or diversion of formula quantities of strategic SSNM [security - limited to Category I facilities];
- loss of control and accounting of formula quantities of SSNM [security & safeguards - limited to Category I facilities];
- unauthorized removal of SNM of moderate strategic significance [security - limited to Category I and II facilities];
- loss of control and accounting of SNM of moderate strategic significance [security & safeguards - limited to Category I and II facilities]; and
- loss or unauthorized disclosure of classified information [security].

The NRC staff envisions that the rule language would require each FCF licensee to submit a cyber security plan for NRC review and approval. The NRC staff expects that licensees would conduct an analysis as part of the cyber security plan to determine the initial set of digital assets – those associated with a consequence of concern. Identification of these digital assets can be informed by commitments used to meet the risk-informed regulations in 10 CFR Parts 40, 70, 73, and 74. Examples of commitments that may inform the proposed cyber security plan include:

- IROFS required to prevent or mitigate significant exposure events (exposures in excess of the performance requirements) that could endanger the life of workers or could lead to irreversible or other serious, long-lasting health effects to workers or members of the public;
- IROFS required to prevent nuclear criticalities. Criticalities are events in which large quantities of radiation are released and could endanger the life of workers (i.e., significant radiation exposures);
- physical security and safeguards programs required to prevent the loss/theft/diversion of significant quantities of SNM. The requirements in the regulations are based on the protection of specific SNM quantities and type of category of facility (i.e., Category I, II, and III); and
- information security programs required to prevent the loss/theft of classified information, which if compromised, could cause damage to the United States.

In considering digital assets associated with safety, a licensee may utilize its ISA to help inform its selection of appropriate digital assets. However, the scope of digital assets that may require cyber security protection could extend beyond those identified with the aid of the ISA, because the ISA requirements in 10 CFR 70.62 do not require consideration of a malicious act and do

not identify controls necessary to prevent a cyber attack from resulting in a consequence of concern. Additional analysis may be needed to identify digital assets associated with operational and process safety functions that, if compromised by a malicious act, could immediately cause a safety consequence of concern. Further evaluation of this topic is expected during rulemaking. It is expected that the rulemaking would limit the identification of digital assets to only those associated with a consequence of concern. It is not the intent of the NRC staff to require FCF licensees to consider 3S digital assets that have no associated consequence of concern.

In considering digital assets associated with security and safeguards, a licensee may utilize its physical security and MC&A programs. Category I FCFs have specific regulatory requirements related to the protection and control of SSNM (10 CFR 73.20 and 74.51) and Category II FCFs have specific regulatory requirements related to protection and control of SNM of moderate strategic significance (10 CFR 73.67 and 74.41). Physical security requirements are in place at enrichment and fuel fabrication (Category III) facilities, and some 10 CFR Part 40 facilities, for several reasons:

- protection of SNM (10 CFR Part 73),
- protection from radiological or chemical consequences (ICM/ASM Orders), and/or
- protection of classified information and components (10 CFR Part 95).

The cyber security consequences of concern currently under consideration by the NRC staff could apply lower thresholds than the radiological or chemical consequences considered by physical security in the ICM Orders for Category III facilities because:

- Category III facilities have a large number of digital controls in place to prevent chemical and radiological consequences, including nuclear criticality.
- A cyber attack is easier than a physical attack to implement –
 - more frequently attemptable,
 - requires less coordination,
 - performed with less resources,
 - low risk of bodily harm to the actor, and
 - exploitable pathways often occur with advancements in technology.
- Based on observations from recent site visits, FCF licensees have implemented digital technologies without fully understanding the cyber threat environment, performing the appropriate cyber security analysis, and applying sufficient cyber security controls.

Category III FCF licensees are required to have graded physical security measures commensurate with the level of risk identified for these facilities (i.e., unauthorized access and various potential consequences). NRC staff is developing a rulemaking that utilizes a similarly graded cyber security approach for protection of certain digital assets commensurate with the risk associated with the compromise of those assets (i.e., cyber attack causing a consequence of concern).

The NRC staff anticipates that the guidance associated with the regulatory requirements would further risk-inform the asset identification process by providing: (1) a screening methodology to account for digital assets whose equivalent 3S function may be provided by an alternate means (i.e., identify a barrier to prevent a consequence of concern from the cyber attack), and (2) a graded technique to apply cyber security controls based on the level of risk associated with the 3S function for the specific facility type. The goal of the planned screening methodology would be to identify the initial set of digital assets (those associated with 3S functions) and refine the scope to those digital assets that would require protection under the new proposed cyber security requirements. The application of cyber security controls would then be limited to this subset of digital assets. The graded technique would then apply only those cyber security controls needed to protect each type of digital asset from compromise, based upon the asset's 3S risk significance. Including a screening methodology and a graded technique in the guidance document would show one method of meeting the anticipated regulatory requirements, while also demonstrating an approach that reduces regulatory burden.

The proposed approach would not require the existing ISAs, physical or information security plans, or MC&A plans to be modified as a result of these new requirements. An FCF licensee's existing ISA, security plan, and MC&A plan could be utilized to inform the cyber security program, i.e., identify which controls that were within the scope of the requirements as well as to inform the screening process. The application of cyber security controls would prevent compromise of the digital assets, therefore further assuring their availability and reliability to perform their intended 3S functions.

The proposed rulemaking would consider using nationally recognized and consensus standards (e.g., NIST SP 800-37, Rev. 1, NIST SP 800-53, Rev. 4, NIST SP 800-82, Rev. 2, "Guide to Industrial Controls Systems Security," and other equivalent standards) when addressing the protection of 3S functions. Selection and application of controls would be driven by factors such as attack vectors and potential consequences. In some cases, existing measures may be credited towards the overall cyber security protection scheme. For example, FCF licensees may be able to take credit for existing physical barriers and access control systems from the physical security program to mitigate certain attack vectors, thereby eliminating the need to apply certain cyber security controls.

4.4 Resolution

The NRC staff envisions a rulemaking that would: (1) be informed by the rule language from 10 CFR 73.54; and (2) address the various types of FCF licensees by implementing a graded approach, based on the consequences of concern by facility type, for the identification (screening) and protection (application of controls) of digital assets. The proposed rulemaking would also build upon current voluntary actions and initiatives undertaken by FCF licensees. The rulemaking, in conjunction with these voluntary actions, is intended to establish a flexible, robust cyber security framework requiring licensees to develop a cyber security program that the NRC staff expects would include the following elements and best practices:

4.4.1 Formation of a CST

The NRC staff anticipates that the licensee's cyber security program would require the establishment of a CST that has authority and independence from plant operations to conduct an objective assessment of cyber security controls, make cyber security determinations and recommendations that are not constrained by operational goals (e.g., cost), and ensure that the

licensee implements protective measures, as required by the proposed rule, to protect against cyber attacks. Roles, responsibilities, authorities, and functional relationships would be expected to be defined and documented to ensure that they are understood by site organizations and individuals (including employees, contractors, temporary employees, visiting researchers, and vendor representatives).

4.4.2 Training staff on cyber security

The NRC staff anticipates that the licensee’s cyber security program would require that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training necessary to effectively perform their assigned duties and responsibilities.

A cyber security control referenced in NIST SP 800-53, Rev. 4, states that cyber security training should be provided for employees to maintain awareness of new threats and employ best practices to reduce the potential for exploitation through attack vectors such as phishing attacks and social engineering techniques. In addition, cyber security training keeps designated personnel updated on current threats, vulnerabilities, and exploits in order to identify key assets affected and apply the latest protection measures or best practices in a timely manner.

4.4.3 Identification of digital assets associated with 3S functions

The NRC staff anticipates that the licensee’s cyber security program would be required to analyze digital computer and communication systems and networks to identify those digital assets associated with 3S functions that must be protected against cyber attacks. The following table represents a conceptual approach under consideration by the NRC staff. The table provides draft thresholds for consequences of concern and an overview of digital assets that the NRC staff expects to consider when defining 3S functions:

Function and (Applicability)	Draft Consequence of Concern	Draft Thresholds	Examples of Digital Assets*
<p>Safety (Apply to all FCF licensees)</p>	<p>Significant exposure events that could endanger the life of workers or could lead to irreversible or other serious, long-lasting health effects to workers or members of the public (e.g., nuclear criticalities and</p>	<p><u>Radiological exposure:</u> - 25 rem or greater worker. - 25 rem or greater or 30 mg or greater intake of uranium in soluble form outside the controlled area (any individual).</p> <p><u>Acute chemical exposure:</u> - Could lead to irreversible or other serious, long lasting health effects to a worker or any individual located outside the controlled area.</p>	<p>Digital assets associated with significant exposure events which may include:</p> <p>- Operational and process controls (i.e., analysis determines that compromise results in a significant exposure event). [Active]</p>

Function and (Applicability)	Draft Consequence of Concern	Draft Thresholds	Examples of Digital Assets*
	releases of radioactive materials or chemicals).		<ul style="list-style-type: none"> - Digital assets associated with preventing and mitigating significant exposure events (e.g., IROFS). [Latent] - Digital assets with a nexus to a significant exposure event (e.g., Security, MC&A). Security digital assets required in response to Security Orders (e.g., ICM, ASM). [Latent]
Security (Apply to Category I FCF licensees)	Radiological Sabotage and Theft or Diversion of Formula Quantities of SSNM.	<p>Loss of the capability to protect against the DBTs as defined in:</p> <ul style="list-style-type: none"> - 10 CFR 73.1(a)(1) Radiological Sabotage. - 10 CFR 73.1(a)(2) Theft or Diversion of Formula Quantities of SSNM. 	<p>Digital assets associated with protecting against the DBTs. [Latent]</p> <ul style="list-style-type: none"> - Security Plans - Security Orders

Function and (Applicability)	Draft Consequence of Concern	Draft Thresholds	Examples of Digital Assets*
<p>Safeguards of SSNM (Apply to Category I FCF licensees)</p>	<p>Loss of control and accounting of Formula Quantities of SSNM.</p>	<p>Loss of the capability to:</p> <ul style="list-style-type: none"> - Timely detect the possible abrupt loss of five or more formula kilograms of SSNM from an individual unit process; - Rapidly determine whether an actual loss of five or more formula kilograms occurred; - Continually confirm the presence of SSNM in assigned locations; and - Timely generate information to aid in the recovery of SSNM in the event of an actual loss. 	<p>Digital assets associated with control and accounting of Formula Quantities of SSNM. [Latent]</p> <ul style="list-style-type: none"> - Security Plans - Fundamental Nuclear Material Control (FNMC) Plan - Security Orders
<p>Security (Apply to Category I and II FCF licensees)</p>	<p>Unauthorized removal of special nuclear material of moderate strategic significance.</p>	<p>Loss of the capability to:</p> <ul style="list-style-type: none"> - Detect, assess and respond to unauthorized access or activities within controlled areas containing SNM of moderate strategic significance. 	<p>Digital assets associated with unauthorized removal of SNM of moderate strategic significance. [Latent]</p> <ul style="list-style-type: none"> - Security Plans - FNMC Plan - Security Orders

Function and (Applicability)	Draft Consequence of Concern	Draft Thresholds	Examples of Digital Assets*
<p>Safeguards of SNM of Moderate Strategic Significance (Apply to Category I and II)</p>	<p>Loss of control and accounting of SNM of moderate strategic significance.</p>	<p>Loss of the capability to:</p> <ul style="list-style-type: none"> - Maintain accurate, current, and reliable information on, and confirm, the quantities and locations of SNM; - Permit rapid determination of whether an actual loss of a significant quantity of SNM has occurred, with significant quantity being either: <ul style="list-style-type: none"> More than one formula kilogram of strategic SNM; or 10,000 grams or more of uranium-235 contained in uranium enriched up to 20.00 percent. - Generate information to aid in the investigation and recovery of missing SNM in the event of an actual loss. 	<p>Digital assets associated with control and accounting of SNM of moderate strategic significance. [Latent]</p> <ul style="list-style-type: none"> - Security Plans - FNMC Plan - Security Orders
<p>Physical Security of Classified Information (Apply to all FCF licensees)</p>	<p>Loss or unauthorized disclosure of classified information.</p>	<p>Loss of the capability to protect classified information.</p>	<p>Digital assets associated with physical security of classified information. [Latent]</p> <ul style="list-style-type: none"> - Standard Practices and Procedures Plan - Security Plans

*The digital assets within scope may also include: support systems equipment which, if compromised, would adversely impact 3S functions; and cyber security features needed to meet commitments in the cyber security program.

Digital assets associated with 3S functions are expected to include those that: (1) perform or are relied upon for 3S functions; (2) could adversely affect 3S functions and/or digital assets that perform 3S functions; (3) provide a pathway to a digital asset that could be used to compromise, attack, or degrade a 3S function; (4) support a digital asset associated with 3S functions (e.g., assets within IROFS boundary package, MC&A assets that provide an input to a digital asset

performing a safety function associated with a consequence of concern, security assets in place to protect against safety consequences of concern, or an asset that could adversely impact the availability, reliability, core functionality, or capability of a 3S function); or (5) protect any of the above from cyber-based attacks.

Concurrent with the regulatory requirements, the NRC plans to publish guidance that would outline a screening methodology which is expected to further reduce the scope of digital assets requiring cyber security controls. The guidance would describe how licensees can take credit for an equivalent 3S function being provided by alternate means. The application of cyber security controls would then be limited to a subset of digital assets, the most risk significant identified by the screening methodology.

4.4.4 Application of cyber security controls to digital assets

The NRC staff anticipates that the licensee's cyber security program would be required to implement cyber security controls for the protection of digital assets that, if compromised, would be associated with a consequence of concern. Recommended baselines of cyber security controls are expected to be included in the guidance document and be similar to those found in nationally recognized cyber security standards (e.g., NIST SP 800-53, Rev. 4).

Furthermore, the NRC staff's current approach is to utilize a graded technique to apply cyber security controls based on the level of risk associated with the function for the specific facility type. The NRC staff is considering development of an impact assessment matrix that would bin digital assets by 3S function into impact categories based on facility type. This graded technique would then apply only those cyber security controls needed to protect each type of digital asset from compromise (i.e., corresponding baseline of cyber security controls). The NRC staff expects the draft rule language to reflect these differences in risk profile and include detail on the identification of these digital assets.

To avoid dual regulation, the NRC staff expects that the rulemaking would specifically exclude these classified systems, and potentially some unclassified systems, if the digital assets are provided with a level of protection equivalent to the NRC rule and are accredited by another federal government entity.

4.4.5 Configuration management

The NRC staff anticipates that the licensee's cyber security program would be required to include a configuration management element that would ensure changes (e.g., configuration, settings, software updates, hardware updates, etc.) to digital assets associated with 3S functions are planned, reviewed, analyzed, and tested prior to implementation in the field. Licensees may be required to develop, disseminate, review, and update a formal, documented configuration management policy and associated implementing procedures. The NRC staff's current approach is for a licensee to document configuration management policy as a part of the facility's existing configuration management program and include hardware configurations, software configurations, and access permissions. Changes to hardware or software could then be documented and accessed in accordance with these policies and implementing procedures.

4.4.6 Cyber security incident response capability

The NRC staff anticipates that the licensee's cyber security program would be required to establish a cyber security incident response element designed to identify, respond, and recover from cyber attacks and other cyber-related incidents. A cyber security program should be designed to mitigate the adverse effects of cyber attacks and ensure that within scope digital assets are not adversely affected. Incident response and recovery measures may be required to accomplish the following:

- maintain the capability for prompt detection and response to cyber attacks;
- mitigate the consequences of cyber attacks prior to adverse impact;
- correct exploited vulnerabilities; and
- restore digital assets and/or support systems affected by cyber attacks.

4.4.7 Cyber security event reporting and recordkeeping

The NRC staff anticipates that the licensee's cyber security program would be required to include a cyber security event notification element that would serve to notify the NRC within a specified timeframe of any cyber attacks that resulted or could have resulted in a consequence of concern. It is expected that, where possible, the cyber security reporting requirements would align with existing reporting requirements currently required by regulation for FCF licensees. Notifications and written reports generated by FCF licensees may be used by the NRC to respond to emergencies, monitor ongoing events, assess trends and patterns, identify precursors of more significant events, and inform other NRC licensees of cyber security-related events, enabling them to increase their security posture or take preemptive actions, if necessary. In addition, timely notifications assist the NRC in achieving its strategic communications mission by informing DHS and Federal intelligence and law enforcement agencies of cyber security-related events that could: (1) endanger public health and safety or the common defense and security, (2) provide information for threat-assessment processes, or (3) generate public or media inquiries.

4.5 Summary

The NRC staff concludes that a cyber security rulemaking would provide additional assurance of a licensee's capability to protect their facility against cyber attacks (up to and including the DBT for Category I fuel facilities) that could cause a consequence of concern. In recognition of advancing digital technology, the proposed rulemaking would expand upon previous security orders by establishing the requirement for a cyber security program to protect any digital assets that, if compromised, could cause a consequence of concern. As licensees implement digital upgrades for many systems at their plants, the potential for adverse consequences from cyber security threats will increase. The NRC staff expects the proposed cyber security rulemaking would minimize the risk of a cyber attack from resulting in a consequence of concern thereby increasing the overall safety and security for FCF licensees. This effort is consistent with the Commission's direction through the SRM to SECY-14-0147 for the NRC staff to implement cyber security requirements necessary to ensure that FCF licensees protect the health and safety of the public and are in accord with the common defense and security.

Chapter 5 Alternatives to Rulemaking Considered

This chapter discusses the alternatives to a rulemaking that the staff considered to resolve the regulatory issues presented in Chapter 3 of this document. This chapter explains why the NRC cannot take actions to resolve the issues effectively within the existing regulatory framework without rulemaking. The alternatives considered are described and the reasons why they were not pursued are discussed.

In summary, none of the considered alternatives completely resolve the identified regulatory issues discussed in Chapter 3 of this document

5.1 No Action

Under this alternative, the staff would rely on existing orders, associated guidance, and voluntary actions to address cyber security concerns for FCF licensees. The NRC would not issue new orders or engage in a rulemaking to address these concerns. The NRC would continue to rely on the 2002–2003 ICM Orders and the 2007 revision to the DBT to address cyber security concerns for FCF licensees. Licensees may or may not implement voluntary actions on an ad hoc basis. The inadequacies of the existing orders, associated guidance, and voluntary initiatives are discussed below.

5.1.1 Timing and Resources

The “no action” alternative would not require any additional resources from NRC staff or FCF licensees. The NRC staff would not engage in the development of new orders. The staff would not need to expend any time and resources on developing a rulemaking and associated guidance to address cyber security concerns for FCF licensees, nor would FCF licensees need to implement any rulemaking requirements.

5.1.2 Stakeholder Interactions

The “no action” alternative would not require new stakeholder interaction.

5.1.3 Regulatory Stability and Enforceability

Under the “no action” alternative, the 2002–2003 ICM Orders and the 2007 revision to the DBT regulations would provide the only cyber security requirements for FCF licensees. However, the inadequacies of the current regulatory framework allow for cyber security vulnerabilities at FCF licensees that may be exploited by an adversary. The risk from the persistent, evolving cyber security threat is expected to increase over time if adequate controls are not established to protect from that threat.

The existing ICM Orders and revised DBT only require that licensees evaluate and address cyber security “as necessary.” The NRC has not provided any specificity or guidance on how licensees are to implement cyber security controls to address the cyber security threat. Consequently, FCF licensees have adopted ad hoc voluntary actions that do not consider certain cyber security vulnerabilities at various types of FCF licensees.

Licensee voluntary actions do not constitute a regulatory framework for addressing cyber security threats to FCF licensees. In addition, the voluntary actions do not provide an analysis

or complete set of controls for digital assets, which could leave facilities susceptible to potential vulnerabilities. Finally, these voluntary actions are not enforceable unless licensees incorporate them into their security plans.

The NRC staff concludes that a rulemaking would establish a predictable regulatory framework to address cyber security threats for FCF licensees. This regulatory framework would improve regulatory stability, allow the NRC to develop and implement appropriate graded, consequence-based requirements for the various types of FCF licensees, and develop related guidance for implementing these requirements. Additionally, a rulemaking would enable the NRC to develop an effective inspection program, reduce regulatory uncertainty, and address enforceability issues.

5.1.4 Summary

Currently, there is no comprehensive regulatory framework for addressing cyber security for FCF licensees. Accordingly, there is no requirement that FCF licensees systematically evaluate, identify, and address cyber security vulnerabilities at their facilities. Approaches vary widely among licensees, lack NRC oversight, and based on prior staff assessments, do not adequately address all attack vectors. Therefore, the NRC staff concludes that the “no action” alternative would not adequately address cyber security threats to FCF licensees. Additionally, the “no action” alternative would not comply with the Commission’s direction in the SRM to SECY-14-0147 to initiate a rulemaking to address cyber security threats for FCF licensees. For these reasons, the NRC staff does not support the “no action” alternative.

5.2 Issue Cyber Security Orders

Under this alternative, the NRC would issue security orders to licensed facilities to implement a cyber security program. This option was presented to the Commission in SECY-14-0147, which included a draft security order that specified requirements for a CST, cyber security awareness training, incident response capabilities, portable media controls, baseline inventory of digital assets, isolation of specific assets, development of applicable cyber security configuration management controls, and the reporting of certain cyber security events. More fulsome orders that require a full cyber security program could be considered.

5.2.1 Timing and Resources

The time and resources required to develop security orders for FCF licensees would be significant. Orders can typically be issued quickly and require fewer resources than the time and resources needed for conducting a rulemaking. However, the development of orders for all applicable facilities could potentially result in a significant cumulative effort for the NRC. Depending on the type of order (generic or facility-specific), multiple interactions between the NRC and each licensee may be required. The NRC would need to analyze site-specific conditions at each facility to determine the appropriate cyber security controls needed, then further consider if these controls are generic among FCF licensees or if a specific order is needed for each licensee. In addition, over time, new applicants may require development of additional orders. Therefore, completing orders for all applicable licensees may be more time-consuming than a rulemaking.

Development of security orders would likely be equally resource intensive for licensees as required for a rulemaking. In addition, the NRC would require fewer resources to develop a single rulemaking than multiple orders, each with site-specific requirements.

Although orders may be preferred for a limited number of licensees or when implementing similar requirements for multiple licensees, a rulemaking is advantageous for overall timing and resources of both the NRC and licensees for cyber security which impacts all FCF licensees and involves site-specific requirements. A rulemaking would also address new licensees.

5.2.2 Stakeholder Interactions

Order development does not involve the same level of stakeholder interactions as required for rulemakings. Rulemakings involve multiple public meetings, comment periods and requests for comment from the public, other government agencies, tribes, and the entire regulated industry. Orders, on the other hand, have a more limited opportunity for stakeholder interaction, other than direct interaction between the NRC and the licensee. As a result, rulemakings receive much more scrutiny and opportunity for improvement based on additional stakeholder feedback. As mentioned above, the increased review and comment by multiple stakeholders reduces the burden to review and comment that would be placed on a single licensee during development of an order.

Additionally, the only stakeholder input that NRC has received on any of the potential options came from NEI, who indicated the preference for a rulemaking over orders in its July 3, 2013, letter on FCF cyber security (not publicly available because it contains security-related information, ADAMS Accession No. ML14174B231). The following is a non-sensitive excerpt from the referenced letter:

Further, the Commission's preference to use rulemaking is also reflected in its direction to the staff with respect to the ongoing "cumulative effects of regulation" effort and its strong endorsement of the agency's efforts to improve its regulatory efforts by increasing and improving opportunities for stakeholder input. Therefore, NRC should proceed to develop a regulatory basis, proposed rule and draft guidance consistent with the agency's current rulemaking processes rather than issuing orders. Unlike the adjudicatory order development process, rulemaking affords a level of stakeholder transparency ideally suited to analyze and resolve the technical issues associated with developing a new regulatory construct and could be completed in a timely manner without undue risk to public health and safety and common defense and security.

We support a methodical regulatory approach to cyber security that is risk-informed – focusing on those systems directly associated with protecting public health and safety. The safety of the public, our workers, and the environment is our number one objective, which we believe would be best achieved by protecting those digital assets whose compromise would directly challenge a licensee's operational safety and security, resulting in a consequence of concern.

5.2.3 Regulatory Stability and Enforceability

Orders provide an enforceable regulatory approach to implement cyber security requirements for FCF licensees. However, because cyber security requirements should be graded commensurate with the level of risk and potential consequences at specific types of facilities,

each facility would likely have a unique set of order requirements. Utilizing a site-specific approach to developing cyber security orders does not promote regulatory predictability or consistency and would not address new applicants/licensees.

5.2.4 Summary

The option to issue orders was presented to the Commission in SECY-014-0147. The Commission directed the NRC staff to proceed with a rulemaking rather than develop orders, a position that stakeholders supported. Based on the lack of significant changes in the threat environment, risk insights discussed above, and large number of resources required, the staff does not recommend the orders alternative.

5.3 Issue Generic Communications

Under this alternative, the NRC could try to use generic communications to explain what it expects licensees to do to address cyber security threats to FCF licensees. There are six types of generic communications NRC could develop and issue. Of these, only Bulletins and Generic Letters require a licensee response; however they are not typically viewed as an appropriate method for addressing emerging regulatory issues absent a clear regulatory framework. The other four generic communications are designed primarily to provide information to licensees.

Bulletins are used to address significant issues having generic applicability that also have great urgency. Bulletins request information from, request specified action by, and require a written response in accordance with Section 182.a of the AEA, from the addressees regarding matters of safety, safeguards, or environmental significance. Addressees may be asked to take compensatory action that is commensurate with the urgency of the issue being addressed, provide requested information, and perform and submit analyses by a specific time. Bulletins may not request long term actions. Bulletins may request new or revised licensee commitments that are based on either NRC or licensee performed analyses and licensee-proposed corrective action. Bulletins may not require license commitments.

Generic Letters are used to request that addressees: (1) perform analyses or submit descriptions of proposed corrective actions regarding matters of safety, safeguards, or the environment and submit, in writing, that they have completed the requests, with or without prior NRC approval of the action; (2) submit technical information that the NRC needs to perform its functions; or (3) submit proposed changes to technical specifications. By a Generic Letter, the NRC may also: (1) provide the addressees with staff technical or policy positions not previously communicated or broadly understood, or (2) solicit addressees' participation in voluntary pilot programs.

5.3.1 Timing and Resources

Generic communications could be issued more quickly and require fewer resources than conducting a rulemaking.

5.3.2 Stakeholder Interactions

Stakeholder interaction would be limited to the possible comment on a draft and the response to a final Bulletin or a Generic Letter. Implementing cyber security as a rulemaking would benefit from increased stakeholder interactions that would not be available through issuance of generic communications.

5.3.3 Regulatory Stability and Enforceability

Generic communications are the NRC's primary method of communicating a common need for information or resolution regarding an issue, or communicating NRC's position and information on issues pertaining to a matter of regulatory interest. Generic communications also allow the NRC to communicate and share industry experiences and send information to specific classes of licensees and interested stakeholders. Generic communications cannot require a licensee to take an enforceable action or make a license commitment. Given their inherent limitations, generic communications do not provide a regulatory framework to implement cyber security for FCF licensees.

5.3.4 Summary

None of the generic communication options would be suitable for addressing the large and complex issues described in Chapter 3 of this document. While they could be used to raise the awareness of the issues discussed in Chapter 3 of this document, these generic communications cannot impose new measures or relax existing requirements on licensees. Additionally, the Commission directed the NRC staff to proceed with a rulemaking in the SRM to SECY-14-0147. Based on the limited impact that generic communications have on the existing regulatory framework, the staff does not recommend this alternative.

5.4 Develop Regulatory Guidance Documents

Under this alternative, the staff would issue guidance rather than carry out a rulemaking. This guidance would rely on new interpretations of existing regulations to identify desired licensee actions.

5.4.1 Timing and Resources

Regulatory guidance documents could be issued more quickly and require fewer resources than conducting a rulemaking. The process for issuing guidance documents is less resource intensive for both the NRC and the industry than a rulemaking.

5.4.2 Stakeholder Interactions

No stakeholder interaction is necessary to develop regulatory guidance documents. Although stakeholder interaction could be requested during the development of regulatory guidance, the stakeholders would likely focus their comments on the existing regulatory framework, similar to the comments presented in Section 5.2.2. Implementing cyber security as a rulemaking would benefit from increased stakeholder interactions that would not be available through the development of regulatory guidance.

5.4.3 Regulatory Stability and Enforceability

Regulatory guides provide guidance to licensees and applicants on acceptable methods for meeting specific parts of the NRC's regulations, techniques used by the staff in evaluating specific issues or postulated accidents, and data needed by the staff in its review of applications for permits or licenses. However, guidance cannot impose new requirements on licensees or mandate licensee action. Additionally, new interpretations of the existing regulatory framework set forth in guidance are generally subject to backfit considerations for those licensees that have backfit provisions in their licensing regulations. Using guidance to implement cyber security

controls to address the threat to FCF licensees could be seen as imposing new requirements without the rulemaking process, in violation of public notice and comment requirements and the NRC's Principles of Good Regulation. Additionally, the NRC would likely need to address backfit concerns.

5.4.4 Summary

Developing regulatory guidance documents, without first undertaking rulemaking, would not be suitable for addressing the large and complex issues described in Chapter 3 of this document. Guidance cannot impose new requirements on licensees, and new interpretations of the existing regulatory framework are subject to backfit considerations. Additionally, the existing regulatory framework does not adequately address all attack vectors and leaves facilities susceptible to potential vulnerabilities. As a result, the risk from the persistent, evolving cyber security threat increases over time if adequate controls are not established through additional orders or a rulemaking. Furthermore, this option is not consistent with the Commission's direction in the SRM to SECY-14-0147 to implement a cyber security rulemaking. Based on the limited impact that developing regulatory guidance has on the existing regulatory framework, the staff does not recommend this alternative.

5.5 Issue Site-Specific License Conditions

Under this alternative, the NRC staff would perform a case-by-case evaluation of each FCF licensee's voluntary cyber security actions and determine whether any additional actions are needed. The NRC staff would then initiate discussions with the FCF licensee to attempt to establish site-specific license conditions in the NRC license that capture all actions needed to adequately address cyber security.

5.5.1 Timing and Resources

Development of site-specific license conditions would likely be as resource intensive for licensees as a rulemaking. In addition, the NRC would require more resources to develop multiple, site-specific license conditions rather than performing a single rulemaking. Unlike a rulemaking where the comments and interactions with the NRC are coordinated by multiple licensees, each interaction for a site-specific license condition would be placed on a single licensee, potentially independent of the other licensees. Sharing the burden to comment and interact with the NRC would reduce the resource burden for licensees during a rulemaking, as compared to the development of site-specific license conditions.

5.5.2 Stakeholder Interactions

Extensive licensee interaction would be required for agreement upon site-specific license conditions. These discussions would be difficult because the existing regulatory framework lacks specific cyber security requirements. Although stakeholder interaction could be requested during the consideration of site-specific license conditions, FCF licensees are under no obligation to agree to modify their licenses. Implementing cyber security as a rulemaking would also benefit from generic stakeholder (i.e., public) interactions that would not be available through the development of site-specific license conditions.

5.5.3 Regulatory Stability and Enforceability

The NRC staff proposes that cyber security requirements should be graded commensurate with the level of hazards, therefore each facility would have unique license conditions. This would create a regulatory burden by requiring each licensee to develop a unique cyber security program without guidance or a regulatory framework. Additionally, because of the unique requirements at each facility, the inspection program would need to be modified for each facility. A rulemaking would allow the NRC to develop a pre-defined, graded, consequence-based regulatory approach. A rulemaking would also allow the NRC to develop industry-wide guidance which would not be possible with license conditions that are unique for each facility.

5.5.4 Summary

Extensive licensee interaction would be required for agreement upon site-specific license conditions. This option has the potential to result in inconsistencies in the requirements and levels of protection among FCF licensees. This option would also create a regulatory burden by requiring the licensees to develop a cyber security program without a comprehensive regulatory framework. This approach would result in a burden on the NRC to review the cyber security programs without established regulatory acceptance criteria. The process of developing and implementing individual license conditions can be time consuming and delay the implementation of cyber security requirements for the protection of SNM. Furthermore, this option is not consistent with the Commission's direction in the SRM to SECY-14-0147 to implement a cyber security rulemaking. Based on the potential challenges present in issuing site-specific license conditions given the existing regulatory framework, the staff does not recommend this alternative.

5.6 Clarify Inspection Modules / Revise Enforcement Guidance

Under these options, inspection modules and/or enforcement guidance would need to be modified to resolve the regulatory issues presented in Chapter 3 of this document. However, without adequate regulatory requirements, the NRC would be unable to revise inspection modules or enforcement guidance. Inspection modules and enforcement guidance cannot create new requirements. No inspection modules or enforcement guidance exist in the current regulatory framework to address cyber security for FCF licensees. The current regulatory framework does not support the creation of new cyber security inspection modules or enforcement guidance for FCF licensees. These options are not applicable.

5.7 Summary

The NRC staff concludes that a rulemaking would establish a predictable regulatory framework to address cyber security threats for FCF licensees. The NRC staff considered alternatives of no action, orders, generic communications, guidance, license conditions, and inspection modules. Each of these approaches was evaluated and determined to have disadvantages when compared to rulemaking. The rulemaking framework would improve regulatory stability, allow the NRC to develop and implement appropriate graded, consequence-based requirements for the various types of FCF licensees, and develop related guidance for implementing these requirements. Additionally, a rulemaking would enable the NRC to develop an effective inspection program, reduce regulatory uncertainty, and address enforceability issues.

Chapter 6 Backfit Rule Applicability

This chapter discusses the applicability of the backfit rule. As discussed in Chapter 1 of this document, the proposed rulemaking would update the physical protection requirements to adopt new cyber security regulations for certain FCF licensees. The specific objective of the proposed rulemaking is to establish new cyber security requirements in 10 CFR Part 73 for FCF licensees to develop, implement, and maintain a cyber security program for the protection of digital computer systems, communication systems, and networks associated with safety, security (physical and information), and safeguards (3S) functions from cyber attacks that could result in the following consequences of concern:

- significant exposure events that could endanger the life of workers or could lead to irreversible or other serious, long-lasting health effects to workers or members of the public (e.g., nuclear criticalities and releases of radioactive materials or chemicals) [safety];
- radiological sabotage and theft or diversion of formula quantities of SSNM [security – limited to Category I facilities];
- loss of control and accounting of formula quantities of SSNM [security & safeguards – limited to Category I facilities];
- unauthorized removal of SNM of moderate strategic significance [security – limited to Category I and II facilities];
- loss of control and accounting of SNM of moderate strategic significance [security & safeguards – limited to Category I and II facilities]; or
- loss or unauthorized disclosure of classified information [security].

Incorporation of the above objective would provide a comprehensive, graded, performance-based regulatory framework to address cyber security vulnerabilities at FCF licensees.

6.1 Entities Accorded Backfit Protection

The proposed rulemaking would apply to FCF license applicants and current FCF licensees who are licensed to possess significant quantities of source material and SNM, including certain 10 CFR Part 40 facilities (e.g., conversion and deconversion) and certain 10 CFR Part 70 facilities (e.g., enrichment, fabrication, and mixed oxide). Of these entities, only FCFs licensed under 10 CFR Part 70 are accorded backfitting protection.

6.2 Future Applicants

Future applicants are not protected by backfitting provisions in 10 CFR 70.76. Backfitting is intended to protect the reasonable expectations of licensees under 10 CFR Part 70, Subpart H, and was not intended to apply to every NRC action that substantially changes the expectations of current and future applicants for licenses under Subpart H.

6.3 10 CFR Part 40 Facilities

FCFs licensed under 10 CFR Part 40 (e.g., uranium hexafluoride conversion and deconversion facilities) are not protected by any backfitting provisions. Therefore, backfitting considerations need not be addressed by the NRC in developing the proposed rule as applied to FCFs licensed under 10 CFR Part 40. However, the NRC would prepare a regulatory analysis that includes consideration of costs and benefits on these facilities.

6.4 10 CFR Part 70 Facilities⁴

FCF licensees which are not subject to the requirements of 10 CFR Part 70, Subpart H, are not protected by the backfit provisions in 10 CFR 70.76, because the backfitting provision in 10 CFR 70.76 applies only to FCF licenses issued under Subpart H. However, the NRC would prepare a regulatory analysis that includes consideration of costs and benefits on the facilities not protected by backfitting under 10 CFR 70.76. The NRC staff anticipates that the cyber security rulemaking would only apply to the 10 CFR Part 70 FCF licensees subject to the requirements of 10 CFR Part 70, Subpart H.

FCF licensees which are subject to the requirements of 10 CFR Part 70, Subpart H, are protected by the backfit provisions in 10 CFR 70.76. The following backfit considerations as applied to FCF licensees subject to 10 CFR Part 70, Subpart H, would be addressed as part of the rulemaking.

6.4.1 Backfitting Defined

Backfitting refers to new regulatory requirements or regulatory staff positions that modify or add to systems, structures, or components of a facility; or to the procedures or organization required to operate a facility. These new requirements or positions may only be imposed on licensees if the NRC justifies the backfit with a backfit analysis (10 CFR 70.76(a)(2)) or explains in a documented evaluation (10 CFR 70.76(a)(4)) why a backfit analysis is not required. Certain categories of regulatory changes are exempt from backfit analysis, or do not fall within the definition of backfitting, as explained below.

6.4.2 Administrative Changes which are Not Subject to Backfit Considerations

Re-sequencing and reorganization of the regulations in 10 CFR Parts 40, 70, and other applicable Parts, which do not include any substantive changes in regulatory requirements, are administrative in nature and do not constitute backfitting as defined in 10 CFR 70.76(a).

6.4.3 Information Collection and Reporting

The rulemaking may involve changes to existing information collection and reporting requirements, or the adoption of new information collection and reporting requirements in 10 CFR Part 73. Information collection and reporting requirements, the primary purpose of which is to support NRC regulatory oversight and not the achievement of substantive regulatory objectives (radiological health and safety or common defense and security), are not subject to

⁴ The rulemaking would not affect 10 CFR Part 70 licensees who are also nuclear power plant licensees under 10 CFR Parts 50 or 52 at the same site where licensed materials are used. Accordingly, the special considerations which apply to such rulemakings are not applicable to this rulemaking.

backfitting consideration. This is a longstanding interpretation of the original Backfit Rule, 10 CFR 50.109, which has been extended to the interpretation of the NRC backfitting provisions in 10 CFR Parts 70, 72, and 76. The rationale underlying the NRC interpretation is that information collection and reporting requirements, by their inherent nature, do not directly provide radiological safety or security benefits. The radiological safety or security benefits associated with information collection and reporting are achieved only through additional NRC regulatory action or licensee action. Hence, the NRC would, in all likelihood, be unable to justify the backfitting of new or changed information collection and reporting requirements which support NRC regulatory oversight.

6.4.4 Codification of Requirements in Orders

Adoption of new or revised regulations which make generically applicable (“codify”) the existing requirements in security orders issued to FCF licensees would not constitute backfitting. Backfitting concerns with respect to the imposition of the requirements in those security orders were addressed as part of the NRC’s issuance of those security orders. Therefore, new or revised regulations which codify the existing security order requirements are not new NRC actions falling within the definition of backfitting. However, to the extent that the new or revised regulations impose additional or substantially changed requirements (as compared with the requirements imposed in the security orders) which cannot be satisfied by a *current* licensee’s/certificate holder’s programs and activities, then those additional or changed requirements would be considered backfitting for existing entities. For such requirements, the NRC would address the applicable backfitting provisions.

6.4.5 Requirements Not Falling into Any Category of Backfitting Rationales

For the proposed regulatory revisions that do not fall into any of the above categories of backfitting rationales, the NRC would need to develop the information necessary to address applicable backfitting requirements in 10 CFR 70.76 in developing any proposed rule. In some cases, an exception from the requirement to prepare a backfit analysis might apply. In other cases, the NRC would need to perform a backfit analysis to determine: (1) whether the applicable option would result in a substantial increase in the overall protection of the public health and safety or the common defense and security, and (2) whether the costs of implementing that option are justified in view of this increased protection.

Chapter 7 Stakeholder Interactions

This chapter discusses stakeholder interactions or other outreach efforts that facilitated development of this regulatory basis document. This chapter also summarizes anticipated stakeholder interactions that are expected to facilitate development of the final regulatory basis document.

7.1 Overview

The staff interacted with licensees, other Federal agencies, and members of the public to obtain supporting information, views, and opinions that are reflected in this regulatory basis. Interactions with potentially affected licensees included FCFs, non-power reactors, and other NRC licensees that possess SNM. Interactions with Federal agencies included the DOE, DHS, NIST, and the National Nuclear Security Administration. Public interaction during development of this regulatory basis was solicited through five announced public meetings held by the NRC staff.

Stakeholder interactions are listed in Attachment A. To increase awareness, solicit input, and facilitate involvement in the development of the regulatory basis, the NRC used the following channels to interact with stakeholders:

1. The NRC has discussed cyber security for FCF licensees with various stakeholders since 2010. The majority of these interactions supported SECY-14-0147 which informed the development of this regulatory basis. The feedback provided on fuel cycle cyber security during the development of SECY 14-0147 is documented in the meeting summaries referenced in Attachment A to this document. These interactions included several meetings with NEI and FCF licensees and four meetings that included other Federal agencies. Most of the meetings were closed to the public given the sensitive, security-related nature of the discussions, although the presentation at the 2012 Fuel Cycle Information Exchange was open to the public (ADAMS Accession No. ML12160A203).
2. The NRC provided the SRM to SECY-14-0147 to FCF licensees to increase awareness of the direction provided to the NRC staff. The SRM to SECY-14-0147 contains sensitive, internal information that is limited to distribution within the NRC unless the Commission determines otherwise.
3. The NRC held public meetings in June 2015 and July 2015 to obtain stakeholder feedback on the major topical areas being considered in this regulatory basis document. These public meetings are further discussed below.
4. The NRC issued a draft of the regulatory basis for public comment on September 4, 2015 (80 FR 53478).
5. The NRC held a public meeting on September 23, 2015, to discuss the draft regulatory basis and technical issues related to the proposed rulemaking. This public meeting is further discussed in the section below.

6. The NRC held public meetings on October 22, 2015, and December 10, 2015, to discuss technical issues associated with the proposed rulemaking. These public meetings are further discussed in the section below.

7.2 NRC Public Meetings Specific to the Regulatory Basis

The staff held announced public meetings on June 12, 2015, and July 13, 2015. The goal of these public meetings was to inform stakeholders on the different aspects of the draft regulatory basis to solicit stakeholder feedback. The NRC staff documented stakeholder feedback in the meeting summaries referenced in Attachment A. Feedback from these public meetings encouraged the NRC staff to clarify the regulatory problem, augment the basis for the proposed changes, and better define the objectives presented in this regulatory basis.

A public meeting was held on September 23, 2015 (soon after the publication of the draft regulatory basis) to discuss the draft regulatory basis and technical issues related to the proposed rulemaking. The NRC staff documented stakeholder feedback in the meeting summary referenced in Attachment A. Feedback from these public meetings encouraged the NRC staff to clarify the scope of the digital assets under consideration by the proposed rulemaking, clearly articulate thresholds for consequences of concern, and further discuss the application of the risk-management framework from NIST SP 800-37, Rev. 1.

Additional public meetings were held on October 22, 2015, and December 10, 2015. The goal of these public meetings was to further inform stakeholders on the technical aspects of the proposed rulemaking. The NRC staff documented stakeholder feedback in the meeting summaries referenced in Attachment A. Feedback from these public meetings encouraged the NRC staff to further clarify the thresholds for consequences of concern, which resulted in some changes to this regulatory basis.

7.3 Comments on the Draft Regulatory Basis

The NRC issued the draft regulatory basis for comments via the *Federal Register* (80 FR 53478; September 4, 2015). The comment period for the document closed on October 5, 2015. A summary of the comments the NRC received and how they were considered can be found in “Comments and NRC Staff Responses on the Draft Regulatory Basis for the Fuel Cycle Cyber Security Proposed Rulemaking” (ADAMS Accession No. ML15355A469).

Chapter 8 Cost/Impact Considerations

This chapter discusses cost and other impacts for the proposed changes presented in Chapter 4 of this document. This chapter discusses potential impacts on three groups: (1) FCF licensees; (2) the NRC; and (3) State, local, or Tribal governments. Potential environmental impacts are also discussed. The analyses presented in this chapter are qualitative and based on the NRC staff's assessment and input from stakeholders. A more detailed cost/impact evaluation would be carried out as part of the Regulatory Analysis in the proposed rule phase.

The NRC staff also considered alternatives to a rulemaking including no action, orders, guidance/generic communications, license conditions, and policy changes. These items are discussed in Chapter 5 of this document. The NRC staff is pursuing rulemaking because it provides a comprehensive regulatory framework, provides opportunity for stakeholder input on the regulatory framework, and implements the Commission's direction in the SRM to SECY-14-0147.

8.1 Applicability

The revision of the cyber security requirements would apply to all FCFs licensed under 10 CFR Part 70 and subject to 10 CFR Part 70, Subpart H (i.e., enrichment facilities, mixed oxide facilities, and fuel fabrication facilities). The requirements would also apply to fuel cycle source material facilities licensed under 10 CFR Part 40 that conduct uranium hexafluoride conversion or deconversion activities.

8.2 Potential Licensee Impacts

As discussed below, the addition of new cyber security requirements and the restructuring of the regulations would result in an increased burden on licensees. The burdens on licensed facilities include the following: (1) conducting an analysis of the facility's 3S systems and support equipment to identify those digital assets that would require additional cyber security measures; (2) establishing an NRC-approved cyber security program which provides the appropriate level of controls, potentially including those applicable from NIST SP 800-53, Rev. 4 (e.g., access control, training, systems protections, etc.); (3) maintaining the cyber security program and configuration management program for new digital assets and modifications; and (4) documentation and event reporting regarding the cyber security program to the NRC.

8.2.1 Establish a Cyber Security Program

Implementation of an NRC-approved cyber security plan would result in added burden for licensees. Licensees would be required to develop a written commitment and description of their cyber security program, then submit it to the NRC for approval. The NRC staff expects that the guidance document would include a template to facilitate the establishment of a cyber security program. The development of a cyber security program may involve adapting any existing voluntary cyber security actions to conform to the new requirements. The program would include establishment of a qualified team that is responsible for implementing cyber controls for required digital assets (i.e., a CST), development of cyber security procedures, and creation of site-wide training requirements. Most licensees have already established a CST through their voluntary initiative.

Through the asset identification process described in the NRC-approved cyber security plan, licensees would conduct analyses to determine assets associated with a potential consequence

of concern from a cyber attack. The analyses would potentially screen out many assets based on specific consequence thresholds. Furthermore, a screening methodology could be applied to screen out the assets whose equivalent function can be provided by an alternate means. Licensees could then further utilize the anticipated guidance to the rule to apply cyber security controls.

Implementation of a cyber security program may identify digital assets that require cyber security controls. This burden would involve evaluating the appropriate cyber controls for application to the assets, documenting this evaluation in a system security plan, and then physically implementing the controls. Examples of potential cyber security controls include documenting existing cyber security qualifications for certain systems (e.g., portable media), development of procedures to prevent use of unauthorized media or hardware (e.g., USB drives), or implementation of controls to isolate key systems from external access (e.g., air gap systems). The level of burden for implementation of the cyber security program would vary by facility due to wide divergence in the depth and effectiveness of voluntary cyber security actions at existing FCF licensees, as well as the number of digital assets requiring cyber security controls.

8.2.2 Maintenance and Configuration Management

The requirement that licensees maintain their cyber security programs over time may present a burden. Some licensees already maintain a configuration management program that would need to be modified to address cyber security considerations – maintain cyber controls; identify new vulnerabilities; assess the cyber security threats for new systems, structures, and components; include cyber considerations in the configuration control program; etc.

8.2.3 Documentation and Event Reporting

The licensee would experience an increased burden to develop, maintain, and submit for NRC review both documentation and reports. The documentation would include initial submittal of the cyber security program via license amendment request, response to requests for additional information, and future amendments to the program. Additional event reporting requirements for cyber security would also apply and require the licensee to notify the NRC when certain criteria have been met. This documentation would need to be maintained in the facility's records consistent with the timeframe(s) specified in the regulations.

8.2.4 Additional Considerations for Licensees

The NRC staff anticipates that the cyber security program would be graded, consequence-based, and provide for a mechanism to screen out digital assets from having to apply cyber controls. As a result, the potential implementation costs would vary among FCF licensees. The grading of the cyber security requirements for assets associated consequences of concern may be based on the type of facility (i.e., Category I FCFs, Category II FCFs, Category III enrichment facilities, Category III fuel fabrication facilities, and uranium hexafluoride conversion and deconversion facilities). This has the potential to reduce the burden on certain categories of facilities – for example, a digital asset performing a security function at a Category I facility would be within scope and may require application of a “high” cyber security control baseline (i.e., control set); however an asset performing a security function at a Category III facility may not require the application of any controls unless the asset has a nexus to safety or if the facility possesses classified information. In addition, the ability to screen out certain digital assets

would provide licensees the flexibility to focus efforts for on the most risk significant digital assets in the areas of safety, security, and safeguards.

The rulemaking is also likely to impose additional NRC inspection requirements for cyber security on FCF licensees. These requirements are expected to be incorporated into existing inspection programs and are anticipated to have limited impact.

Based on comments and discussions provided by industry during the June 11 and July 13, 2015, public meetings, several licensees believe that the proposed approaches and changes to cyber security would have a significant burden because they would result in revisions to the ISA. The NRC staff recognizes that the ISA would be used to inform the cyber security program, but this program would be independent of the ISA and require no revisions to the ISA.

The NRC staff recognizes that many of the measures described in this regulatory basis are conceptual and open to interpretation. However, the NRC staff expects the proposed rule and related guidance development associated with the proposed rule would clarify the scope of these proposed requirements. The NRC staff expects that stakeholders would be provided draft rule language as it develops and have the opportunity to comment on proposed rule language and guidance documents.

8.3 Impact on the NRC

8.3.1 Rulemaking

The NRC's development and implementation of cyber security regulations through a rulemaking represents an increased burden for the NRC. The agency has committed a significant number of technical staff to developing the rulemaking and related guidance over a 3-year period. The bulk of this burden would occur during the rulemaking process, but some minor additional costs would be associated with keeping the guidance up to date on a periodic basis.

8.3.2 NRC Oversight

Review of the licensees' implementation of cyber security requirements would result in an increased burden for the NRC. The agency would be responsible for reviewing and approving the licensees' cyber security programs. This would require NRC staff in licensing and security to review documentation and may involve site visits for first hand evaluation. The NRC staff would need to incorporate cyber security into the inspection program. NRC inspectors may also need training to evaluate compliance with the cyber security program and take adequate enforcement actions as necessary.

8.4 Impact on State, Local, or Tribal Governments

The proposed changes are unlikely to affect local, State, or tribal government resources. Agreement State authorities would not be required to adopt a similar requirement for their licensees because quantities of SNM and source material that could be regulated by an Agreement State are not subject to the proposed cyber security requirements. As a result, State and local resource needs would be unaffected.

8.5 Environmental Analysis

During the proposed rule phase, the proposed rule language would be analyzed for its potential effects on the environment. The current intent is for the proposed rule language to concern only cyber security, with no impact to licensed activities involving source material or SNM. The NRC does not anticipate that the rule would have any significant impact on the environment.

8.6 Cost Justification

A rulemaking to implement cyber security requirements for FCF licensees would have a number of benefits that justify the potential cost impacts both on the licensee and the NRC. Cyber security attacks by malicious actors have the potential to compromise important information, disable or degrade security systems, and compromise or reduce the reliability of critical safety systems. Although licensees recognize and have implemented some voluntary actions to address cyber security, significant gaps exist in the rigor of the onsite analyses, controls implemented, and implementation of cyber security programs. The NRC concludes that the costs associated with a cyber security rulemaking would be offset by the benefits to public health and safety and the common defense and security, gained from protecting against cyber attacks on FCF licensees that could result in consequences of concern related to safety, security, and safeguards, including:

- significant exposure events that could endanger the life of workers or could lead to irreversible or other serious, long-lasting health effects to workers or members of the public (e.g., nuclear criticalities and releases of radioactive materials or chemicals) [safety];
- radiological sabotage and theft or diversion of formula quantities of SSNM [security – limited to Category I facilities];
- loss of control and accounting of formula quantities of SSNM [security & safeguards – limited to Category I facilities];
- unauthorized removal of SNM of moderate strategic significance [security – limited to Category I and II facilities];
- loss of control and accounting of SNM of moderate strategic significance [security & safeguards – limited to Category I and II facilities]; or
- loss or unauthorized disclosure of classified information [security].

A cyber security program that meets these requirements is necessary for FCF licensees to ensure the health and safety of the public and the common defense and security.

Chapter 9 NRC Strategic Plan

The NRC's mission is to regulate the Nation's civilian use of byproduct, source, and SNM to protect public health and safety, to promote the common defense and security, and to protect the environment. The NRC's Strategic Plan describes how the NRC plans to achieve its two strategic goals:

- Safety: Ensure the safe use of radioactive materials; and
- Security: Ensure the secure use of radioactive materials.

The NRC's two strategic goals are the results the agency must achieve to successfully carry out its mission. This chapter explains how the recommended action would support the NRC's Strategic Plan goals, as well as their associated implementation strategies.

To achieve the safety strategic goal, the NRC developed the following safety-goal implementation strategies designed to minimize the likelihood of accidents and reduce the consequences of an accident (should one occur).

1. Enhance the NRC's regulatory programs as appropriate using lessons learned from domestic and international operating experience and other sources.
2. Enhance the risk-informed and performance-based regulatory framework in response to advances in science and technology, policy decisions, and other factors.
3. Ensure the effectiveness and efficiency of licensing and certification activities to maintain both quality and timeliness of licensing and certification reviews.
4. Maintain effective and consistent oversight of licensee performance to drive continued licensee compliance with NRC safety requirements and license conditions.
5. Ensure the NRC's readiness to respond to incidents and emergencies involving NRC-licensed facilities and radioactive materials and other events of domestic and international interest.
6. Ensure that nuclear facilities are constructed in accordance with approved designs and that there is an effective transition from oversight of construction to oversight of operation.
7. Ensure that the environmental and site safety regulatory infrastructure is adequate to support the issuance of new nuclear licenses.

To achieve the security strategic goal, the NRC developed the following security-goal implementation strategies designed to prevent hostile damage to nuclear facilities that could cause a significant release of radioactive material to the environment and to avoid instances in which radioactive materials are used in a malevolent manner.

1. Ensure the effectiveness and efficiency of the regulatory framework using information gained from operating experience and external and internal assessments in response to technology advances and changes in the threat environment.
2. Maintain effective and consistent oversight of licensee performance to drive licensee compliance with NRC security requirements and license conditions.
3. Support U.S. national security interests and nuclear nonproliferation policy objectives within NRC's statutory mandate through cooperation with domestic and international partners.
4. Ensure MC&A for SNM.
5. Protect critical digital assets.
6. Ensure timely distribution of security information to stakeholders and international partners.
7. Ensure that programs for the handling and control of classified and safeguards information are effectively implemented at the NRC and licensee facilities.

The actions proposed in this regulatory basis support the NRC's Strategic Plan primarily in safety implementation strategies 1 and 2 and security implementation strategies 1, 3, 4, and 5.

Safety implementation strategy 1 directs that enhancements to the NRC's regulatory programs be based on lessons learned from domestic and international operating experience and other sources. The development of cyber security requirements for FCF licensees is expected to be informed by lessons learned from implementation of the 10 CFR 73.54 power reactor cyber security rule and related guidance. Additionally, the development of cyber security requirements for FCF licensees is expected to be informed by the extensive stakeholder interaction that occurred during the development and implementation of the power reactor cyber security rule as well as subsequent stakeholder interaction with FCF stakeholders, including staff participation in appropriate industry meetings and conferences. Finally, the staff intends to use appropriate national and international consensus standards as an acceptable means of implementing the proposed requirements. The use of these consensus standards takes into consideration domestic and international operating experience and best practices.

Furthermore, as part of this rulemaking effort, the staff reviewed and considered the International Atomic Energy Agency (IAEA) guidance identified in Information Circulars (INFCIRC) INFCIRC/225, Revision 5, "Nuclear Security Recommendations on Physical protection of Nuclear Material and Nuclear Facilities." The NRC supports the United States government's efforts to promote implementation of this document internationally and, as appropriate, seeks to ensure consistency in its own programs. The document provides general guidance on the cyber protection of computer-based safety and security systems. The staff also considered the guidance in IAEA Nuclear Security Series No. 17, "Computer Security at Nuclear Facilities," and draft guidance document NST036, "Computer Security of Instrumentation and Control Systems at Nuclear Facilities."

The staff's proposed approach for developing cyber security requirements for FCF licensees supports safety implementation strategy 1.

Safety implementation strategy 2 directs that enhancements to the NRC's regulatory programs be risk-informed and performance-based. The development of cyber security requirements is expected to utilize a graded, risk-informed, performance-based approach to identify and implement appropriate cyber security controls, taking into account differences among types of FCF licensees and the potential consequences of concern associated with each type of facility. The NRC staff is of the opinion that this approach would result in a predictable and stable regulatory framework to implement cyber security requirements for FCF licensees consistent with the Commission's policy direction in the SRM to SECY-14-0147.

The staff's proposed approach for developing cyber security requirements for FCF licensees supports safety implementation strategy 2.

Security implementation strategy 1 directs that information gained from operating experience and changes in the threat environment be used to ensure the effectiveness and efficiency of the NRC's regulatory framework. As previously discussed in Chapter 3 of this document, the NRC does not currently have an efficient and effective regulatory framework to implement cyber security requirements for FCF licensees. Based on information gained during the 2011 and 2014 cyber security assessments of voluntary actions taken by FCF licensees, the NRC staff determined that there are digital assets susceptible to potential attack vectors that require additional analysis and cyber security protection. Additionally, the staff has worked with other Federal partners, including liaisons within the intelligence community and law enforcement, to assess and understand changes in the threat environment. The staff has further facilitated interactions between DHS and licensees to increase licensee understanding of the threat environment. The NRC staff has concluded that this information is critical in developing an efficient, effective, and consistent regulatory framework to implement cyber security requirements for FCF licensees.

The staff's proposed approach for developing cyber security requirements for FCF licensees supports security implementation strategy 1.

Security implementation strategy 3 directs that cooperation with domestic and international partners will support United States national security interests and nuclear nonproliferation policy objectives within NRC's statutory mandate. The interactions discussed below occurred prior to and during the development of this regulatory basis. These interactions would inform the staff's efforts in establishing cyber security requirements for FCF licensees. The staff expects that these requirements would address security of digital assets associated with physical security, information security, and MC&A programs (i.e., safeguards aspects), each of which play a significant role in supporting national security and nuclear nonproliferation.

The NRC staff frequently interact with staff from DHS ICS-CERT regarding cyber events and new threats. The staff also support efforts by the IAEA to develop technical guidance on computer security at nuclear facilities and recently participated in an IAEA sponsored conference, "International Conference on Computer Security in a Nuclear World."

The staff also considered actions taken by other Federal agencies in protecting digital technologies to determine the best approach to establishing the requirements for FCF

licensees. The staff evaluated the cyber protection programs in place at the DOE, DHS, Federal Energy Regulatory Commission, and North American Electric Reliability Corporation. The staff has also evaluated the numerous cyber security guidance documents developed by NIST and met with NIST staff involved in the development of the documents.

The staff's proposed approach for developing cyber security requirements for FCF licensees supports security implementation strategy 3.

Security implementation strategy 4 directs that MC&A be ensured for facilities licensed to possess SNM. Based on information gained during the 2011 and 2014 cyber security assessments of voluntary actions taken by FCF licensees, the NRC staff determined that there are safeguards components of MC&A that are susceptible to attack vectors that require additional analysis and cyber security protection. The development of cyber security requirements for FCF licensees is expected to apply a graded and consequence-based approach for determining the appropriate security controls for digital assets associated with MC&A functions. Appropriate cyber controls would protect the integrity of MC&A safeguards functions and help to ensure the SNM is properly accounted for and protected from loss, theft, or diversion.

The staff's proposed approach for developing cyber security requirements for FCF licensees supports security implementation strategy 4.

Security implementation strategy 5 requires the protection of critical digital assets. The staff has evaluated the need to address cyber security requirements for FCF licensees. As previously noted, the NRC does not have a have an efficient and effective regulatory framework to implement cyber security requirements for FCF licensees. The ICM Orders and the revised DBT have general performance requirements directing FCF licensees to address cyber security as necessary. These performance requirements do not provide licensees with any direction on how to address cyber security. Furthermore, there is no effective guidance for licensees addressing this issue. Based on information gained during the 2011 and 2014 cyber security assessments of voluntary actions taken by FCF licensees, the NRC staff determined that there are digital assets susceptible to potential attack vectors that require additional analysis and cyber security protection. The development of cyber security requirements for FCF licensees is expected to apply a graded and consequence-based approach for the protection of critical digital assets associated with safety, security (both physical security and classified information security), and safeguards. These requirements would result in an effective and comprehensive set of controls that helps ensure that these critical digital assets are available when needed and would perform reliably, as intended and required by NRC regulations.

The staff's proposed approach for developing cyber security requirements for FCF licensees supports security implementation strategy 5.

Chapter 10 Guidance Documents

This chapter discusses the potential impact the rulemaking may have on NRC guidance documents and inspection programs.

10.1 New Guidance Documents

A new RG would be developed to describe an acceptable approach for FCF licensees to implement the cyber security requirements in the proposed rule. The RG would cover Category I, II, and III FCFs licensed under 10 CFR Part 70 and uranium hexafluoride conversion and deconversion facilities licensed under 10 CFR Part 40. The RG would describe how these facilities should implement a cyber security program to protect digital assets associated with safety, security (physical and information), and safeguards from cyber attacks associated with a consequence of concern. The guidance would also set forth a screening methodology for analyzing the digital assets within the scope of the rule. The draft RG is scheduled to be developed and issued in parallel with the proposed rule.

10.2 Existing Guidance Documents to be Revised

There are no existing guidance documents that would need to be revised to address cyber security for FCF licensees.

10.3 Rescinded Guidance Documents

There are no guidance documents that would need to be rescinded to support cyber security for FCF licensees.

10.4 Inspection Program

The inspection program for FCF licensees (NRC Inspection Manual Chapter 2600) would require a revision to address any new cyber security requirements. Depending on the scope of any new requirements, existing inspection procedures could be modified or a new inspection procedure may need to be established. The NRC staff expects to have a better understanding of any needed modifications to the FCF inspection program as the rulemaking process develops.

Chapter 11 Resources

The rulemaking is being tracked by the Commission. As such, this rulemaking is included in the NRC budget process. Budgeted activities include developing the proposed and final rule packages, stakeholder interaction, guidance development, and development of inspection procedures.

Chapter 12 Timing

In the SRM to SECY-14-0147, the Commission directed the NRC staff to proceed directly with a cyber security rulemaking designated as a high priority and that the final rule should be completed and implemented in an expeditious manner. The proposed rule and associated guidance are scheduled to be submitted to the Commission on or before March 17, 2017. The final rule and associated guidance are scheduled to be submitted to the Commission on or before June 11, 2018. No significant policy or legal issues were identified during the development of this regulatory basis that would need to be resolved before commencing a rulemaking.

Chapter 13 References

AREVA NP, Inc., not publicly available letter (ADAMS Accession No. ML14174B287), July 18, 2012.

AREVA NP, Inc., Comment Letter on Draft Regulatory Basis (ADAMS Accession No. ML15287A413), October 5, 2015.

Atomic Energy Act of 1954, as amended, August 30, 1954.

Babcock & Wilcox Nuclear Operations Group, not publicly available letter (ADAMS Accession No. ML14174B302), July 23, 2012.

BWX Technologies, Inc., Comment Letter on Draft Regulatory Basis (ADAMS Accession No. ML15292A560), October 5, 2015

CB&I AREVA MOX Services, LLC, Comment Letter on Draft Regulatory Basis (ADAMS Accession No. ML15287A417) October 5, 2015.

Chatham House, the Royal Institute of International Affairs, “Cyber Security at Civil Nuclear Facilities Understanding the Risks,” October 2015.

Energy Policy Act of 2005, Title 42 U. S. Code Chapter 149, August 8, 2005.

Global Nuclear Fuels – Americas, Comment Letter on Draft Regulatory Basis (ADAMS Accession No. ML15287A416), October 5, 2015.

Honeywell International, Inc., Comment Letter on Draft Regulatory Basis (ADAMS Accession No. ML15287A414), October 2, 2015.

International Atomic Energy Agency, “Computer Security at Nuclear Facilities,” Technical Guidance Reference Manual, Nuclear Security Series No. 17, December 2011.

International Atomic Energy Agency, “NST036 – Computer Security of Instrumentation and Control Systems at Nuclear Facilities,” Draft Guidance Document, November 2014.

International Atomic Energy Agency, “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities,” INFCIRC/225, Revision 5, Nuclear Security Series No. 13, January 2011.

International Atomic Energy Agency, Office of Public Information and Communication, “Secure Computer Systems Essential to Nuclear Security, Conference Finds,” June 8, 2015.

National Institute of Standards and Technology, Special Publication 800-37, Revision 1, “Applying a Risk Management Framework,” February 2010.

National Institute of Standards and Technology, Special Publication 800-53, Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations,” April 2013.

National Institute of Standards and Technology, Special Publication 800-82, Revision 2, "Guide to Industrial Controls Systems Security," May 2015.

Nuclear Energy Institute, not publicly available letter (ADAMS Accession No. ML14174B279), July 10, 2012.

Nuclear Energy Institute, not publicly available letter (ADAMS Accession No. ML14174B272), January 17, 2013.

Nuclear Energy Institute, not publicly available letter (ADAMS Accession No. ML14174B231), July 3, 2013.

Nuclear Energy Institute, not publicly available letter (ADAMS Accession No. ML14174B308), May 19, 2014.

Nuclear Energy Institute, Comment Letter on Draft Regulatory Basis (ADAMS Accession No. ML15355A448), October 5, 2015.

Nuclear Fuel Services, Inc., Comment Letter on Draft Regulatory Basis (ADAMS Accession No. ML15292A559), October 5, 2015.

Title 10, "Energy," of the Code of Federal Regulations, Part 20, "Standards for Protection Against Radiation."

Title 10, "Energy," of the Code of Federal Regulations, Part 25, "Access Authorization."

Title 10, "Energy," of the Code of Federal Regulations, Part 40, "Domestic Licensing of Source Material."

Title 10, "Energy," of the Code of Federal Regulations, Part 70, "Domestic Licensing of Special Nuclear Material."

Title 10, "Energy," of the Code of Federal Regulations, Part 73, "Physical Protection of Plants and Materials."

Title 10, "Energy," of the Code of Federal Regulations, Part 74, "Material Control and Accounting of Special Nuclear Material."

Title 10, "Energy," of the Code of Federal Regulations, Part 95, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data."

URENCO USA, Comment Letter on Draft Regulatory Basis (ADAMS Accession No. ML15287A412), October 5, 2015.

U.S. Department of Energy, Office of Inspector General, Audit Report DOE-OIG-16-02, "The Department of Energy's Cyber Security Risk Management Framework," November 2015.

U.S. Department of Homeland Security, Industrial Control Systems – Cyber Emergency Response Team, Alert ICS-ALERT-14-176-02A, June 27, 2014.

U.S. Department of Homeland Security, Industrial Control Systems – Cyber Emergency Response Team, Alert ICS-ALERT-14-281-01B, December 10, 2014.

U.S. Department of Homeland Security, Recommended Practice, “Improving Industrial Control Systems Cyber Security with Defense-In-Depth Strategies,” October 2009.

U.S. Nuclear Regulatory Commission, 2012 Fuel Cycle Information Exchange presentation (ADAMS Accession No. ML12160A203), June 13, 2012.

U.S. Nuclear Regulatory Commission, Closed Meeting Summary of August 30, 2011, not publicly available (ADAMS Accession No. ML12026A053).

U.S. Nuclear Regulatory Commission, Closed Meeting Summary of January 9, 2012, not publicly available (ADAMS Accession No. ML12020A095).

U.S. Nuclear Regulatory Commission, Closed Meeting Summary of October 3, 2013, not publicly available (ADAMS Accession No. ML13280A467).

U.S. Nuclear Regulatory Commission, “Comments and NRC Staff Responses on the Draft Regulatory Basis for the Fuel Cycle Cyber Security Proposed Rulemaking,” (ADAMS Accession No. ML15355A469), December 22, 2015.

U.S. Nuclear Regulatory Commission, Cyber Security for Fuel Cycle Facilities Working Group Final Report, not publicly available (ADAMS Accession No. ML120900705), February 25, 2012.

U.S. Nuclear Regulatory Commission, Draft Regulatory Basis, “Rulemaking for Cyber Security at Fuel Cycle Facilities,” (80 FR 53478), September 4, 2015.

U.S. Nuclear Regulatory Commission, Final Rule, “Design Basis Threat” (72 FR 12705), March 19, 2007.

U.S. Nuclear Regulatory Commission, Final Rule, “Power Reactor Security Requirements” (74 FR 13926), March 27, 2009.

U.S. Nuclear Regulatory Commission, Information Assessment 13-02, “Criteria for Reporting Cyber Security Incidents,” not publicly available (ADAMS Accession No. ML13266A214), September 2013.

U.S. Nuclear Regulatory Commission, Inspection Manual Chapter 2600, “Fuel Cycle Facility Operational Safety and Safeguards Inspection Program,” January 27, 2010.

U.S. Nuclear Regulatory Commission, Meeting Presentation of March, 29, 2012 (ADAMS Accession No. ML120870149).

U.S. Nuclear Regulatory Commission, Meeting Summary of March 3-5, 2014 (ADAMS Accession No. ML14072A113).

U.S. Nuclear Regulatory Commission, Meeting Summary of June 11, 2015 (ADAMS Accession No. ML15174A130).

U.S. Nuclear Regulatory Commission, Meeting Summary of July 13, 2015 ADAMS Accession No. ML15208A450).

U.S. Nuclear Regulatory Commission, Meeting Summary of September 23, 2015 (ADAMS Accession No. ML15306A267).

U.S. Nuclear Regulatory Commission, Meeting Summary of October 22, 2015 (ADAMS Accession No. ML15308A506).

U.S. Nuclear Regulatory Commission, Meeting Summary of December 10, 2015 (ADAMS Accession No. ML15356A357).

U.S. Nuclear Regulatory Commission, Regulatory Basis, "Enhanced Security of Special Nuclear Material" (77 FR 22434), April 22, 2015.

U.S. Nuclear Regulatory Commission, Regulatory Guide 5.70, "Guidance for the Application of the Theft Diversion Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.45 and 73.46," not publicly available (Safeguards Information), September 2007.

U.S. Nuclear Regulatory Commission, Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities" (ADAMS Accession No. ML090340159), January 2010.

U.S. Nuclear Regulatory Commission, SECY-12-0088, "The Nuclear Regulatory Commission Cyber Security Roadmap" (ADAMS Accession No. ML12135A050), June 25, 2012.

U.S. Nuclear Regulatory Commission, SECY-14-0147, "Cyber Security for Fuel Cycle Facilities," not publicly available (ADAMS Accession No. ML14177A264), December 30, 2014.

U.S. Nuclear Regulatory Commission, Site Visit Report (ADAMS Accession No. ML15292A098), October 19, 2015.

U.S. Nuclear Regulatory Commission, SRM to SECY-14-0147, "Cyber Security for Fuel Cycle Facilities" (ADAMS Accession No. ML15083A175), March 24, 2015.

U.S. Nuclear Regulatory Commission, Strategic Plan, NUREG-1614, Volume 6: Fiscal Years 2014-2018 (ADAMS Accession No ML14246A439), August 2014.

U.S. Nuclear Regulatory Commission, Threat Workshop of May 30, 2013 (ADAMS Accession No. ML13168A386), July 26, 2013.

Westinghouse Electric Company, LLC, Comment Letter on Draft Regulatory Basis (ADAMS Accession No. ML15287A415), October 5, 2015.

Attachment A. Outreach Initiatives for Fuel Cycle Cyber Security

Timeline of Stakeholder Interactions

- August 30, 2011 – NRC presentation at a closed NEI meeting, followed by a discussion of gaps in fuel cycle cyber security (ADAMS Accession No. ML12026A053).
- November 30, 2011 – Briefing to representatives from the National Nuclear Security Agency's Naval Reactors Program on potential paths forward and impacts.
- December 6, 2011 – Briefing to representatives from the DOE's Oak Ridge Office on potential paths forward and impacts.
- January 9, 2012 – NRC and NEI discussion at a closed meeting (ADAMS Accession No. ML12020A095).
- January 26, 2012 – NRC and NEI teleconference.
- March 29, 2012 – NRC and NEI discussion at a closed meeting (ADAMS Accession No. ML120870149).
- June 13, 2012 – Public Fuel Cycle Information Exchange presentation (ADAMS Accession No. ML12160A203).
- June 14, 2012 – Classified cyber security threat briefing and progress meeting for licensees followed by an unclassified briefing for licensees on cyber security threat provided by representatives from the DHS, ICS-CERT.
- December 18, 2012 – NRC and NEI teleconference.
- May 30, 2013 – Threat Workshop for licensees that included sensitive, security-related presentations on advanced persistent threat and security of industrial control systems, an expert panel discussion, and three technical demonstrations (ADAMS Accession No. ML13168A386).
- June 13, 2013 – Classified briefing for licensees on cyber security threat provided by representatives from DHS, ICS-CERT.
- October 3, 2013 – NRC and NEI presentations and discussion at a closed meeting (ADAMS Accession No. ML13280A467).
- March 3, 2014 – NRC presentation at a closed meeting, followed by discussion of progress (ADAMS Accession No. ML14072A142).

Licensee Letters to the NRC Regarding Fuel Cycle Cyber Security

- NEI letter dated July 10, 2012 (ADAMS Accession No. ML14174B279).

- AREVA NP, Inc. letter dated July 18, 2012 (ADAMS Accession No. ML14174B287).
- Babcock & Wilcox Nuclear Operations Group letter dated July 23, 2012 (ADAMS Accession No. ML14174B302).
- NEI letter dated January 17, 2013 (ADAMS Accession No. ML14174B272).
- NEI letter dated July 3, 2013 (ADAMS Accession No. ML14174B231).
- NEI letter dated May 19, 2014 (ADAMS Accession No. ML14174B308).
- Stakeholder comments on draft regulatory basis: include in reference section
 - NEI letter dated October 5, 2015 (ADAMS Accession No. ML15355A448).
 - AREVA NP, Inc. letter dated October 5, 2015 (ADAMS Accession No. ML15287A413).
 - BWX Technologies, Inc. letter dated October 5, 2015 (ADAMS Accession No. ML15292A560).
 - CB&I AREVA MOX Services, LLC letter dated October 5, 2015 (ADAMS Accession No. ML15287A417).
 - Global Nuclear Fuels - Americas letter dated October 5, 2015 (ADAMS Accession No. ML15287A416).
 - Honeywell International, Inc. letter dated October 2, 2015 (ADAMS Accession No. ML15287A414).
 - Nuclear Fuel Services, Inc. letter dated October 5, 2015 (ADAMS Accession No. ML15292A559).
 - URENCO USA letter dated October 5, 2015 (ADAMS Accession No. ML15287A412).
 - Westinghouse Electric Company LLC letter dated October 5, 2015 (ADAMS Accession No. ML15287A415).

Stakeholder Interactions Specific to the Fuel Cycle Cyber Security Rulemaking

- June 11, 2015 – Public meeting on cyber security to discuss goals and milestones for the rulemaking (ADAMS Accession No. ML15174A130).
- July 13, 2015 – Public meeting on cyber security to discuss rulemaking goals and site visits (ADAMS Accession No. ML15208A450).
- September 23, 2015 – Public meeting on cyber security to discuss draft regulatory basis and technical aspects of rulemaking (ADAMS Accession No. ML15306A267).
- October 22, 2015 – Public meeting on cyber security to discuss technical aspects of rulemaking (ADAMS Accession No. ML15308A506).
- December 10, 2015 – Public meeting on cyber security to discuss technical aspects of rulemaking (ADAMS Accession No. ML15356A357).