THIS PRELIMINARY PROPOSED RULE LANGUAGE AND ACCOMPANYING DISCUSSION IS BEING RELEASED TO SUPPORT INTERACTIONS WITH STAKEHOLDERS AND THE ADVISORY COMMITTEE ON REACTOR SAFEGUARDS (ACRS). THIS LANGUAGE HAS NOT BEEN SUBJECT TO COMPLETE NRC MANAGEMENT OR LEGAL REVIEW, AND ITS CONTENTS SHOULD NOT BE INTERPRETED AS OFFICIAL AGENCY POSITIONS. THE NRC STAFF PLANS TO CONTINUE WORKING ON THE CONCEPTS AND DETAILS PROVIDED IN THIS DOCUMENT AND WILL CONTINUE TO PROVIDE OPPORTUNITIES FOR PUBLIC PARTICIPATION AS PART OF THE RULEMAKING ACTIVITIES.

THE STAFF IS PRIMARILY SEEKING INSIGHTS REGARDING THE CONCEPTS IN THIS PRELIMINARY LANGUAGE AND SECONDARILY SEEKING INSIGHTS RELATED TO DETAILS SUCH AS NUMERICAL VALUES FOR VARIOUS CRITERIA. WHILE THE NRC WILL CONSIDER ALL COMMENTS RECEIVED IN FURTHER DEVELOPING THE PRELIMINARY LANGUAGE, IT WILL NOT PROVIDE WRITTEN RESPONSES TO THOSE COMMENTS. ONCE THE PROPOSED RULE IS ISSUED IN THE *FEDERAL REGISTER*, THE PUBLIC WILL HAVE AN ADDITIONAL OPPORTUNITY TO PROVIDE COMMENTS AND THE AGENCY WILL RESPOND IN WRITING TO ALL PUBLIC COMMENTS ON THE PROPOSED RULE WHEN ISSUING A FINAL RULE.

STAFF DISCUSSION OF CYBER SECURITY – PRELIMINARY RULE LANGUAGE **(November 2021)**

Preliminary Language	Discussion
CYBER SECURITY	
§ 73.110 - Technology neutral requirements for protection of digital computer and communication systems and networks	The proposed section implements a graded approach to determine the level of cyber security protection required for digital computer, communication systems and networks (i.e., protection at the cyber security program level and the security controls implementation level). A graded approach based on consequences is intended to account for the differing risk levels within reactor technologies. Specifically, the proposed section requires licensees to demonstrate reasonable assurance of protection against cyber attacks commensurate with the potential consequences from those attacks. The

	graded approach will be further explained as part of a new regulatory guidance development effort. The proposed section leverages (1) the operating experience from power reactors and fuel cycle facilities and (2) the 10 CFR 73.54 framework, which contains some of the basic requirements needed for cyber security regardless of type of reactor. Differences between the 10 CFR 73.54 requirements and those discussed herein are primarily based on the implementation of a graded approach to cyber security as discussed above to accommodate the wide range of reactor technologies to be assessed by the NRC.
(a) Each licensee of a commercial nuclear reactor under 10 CFR part 53 shall establish, implement, and maintain a cyber security program that is commensurate with the potential consequences resulting from cyber attacks~~. Accordingly, each licensee shall~~, up to and including the design basis threat as described in § 73.1. The cyber security program must provide reasonable assurance that digital computer and communication systems and networks are adequately protected against cyber attacks that are capable of causing the following consequences:	This paragraph implements a graded approach to cyber security to accommodate the wide range of reactor technologies to be assessed by the NRC. Specifically, this section provides criteria for implementing a consequence-based approach to cyber security by determining whether a potential cyber attack would result in the consequences listed herein. The licensee shall establish, implement, and maintain a cyber security program for protecting those digital assets within the scope of § 73.110 that makes use of risk insights, including threat information, and considers the resulting level of consequences of the threats.
~~(1) Exceeding the criterion in § 53.830(a)(2)(i);~~ (1) Adversely impacting the functions performed by digital assets that prevent a postulated radiological release exceeding the offsite dose values in §§ 53.210(a) and (b) of this chapter.	This consequence deals with a scenario where the cyber attack leads to offsite radiation hazards that would endanger public health and safety (i.e., the resulting consequence exceeds reference dose values in §§ 53.210(a) and (b)).

(2) Adversely impacting the functions performed by ~~the~~ digital assets used by the licensee for implementing the physical security requirements in § 53.830(a)~~)(1~~) of this chapter ~~for special nuclear material, source material, and byproduct material~~.	This consequence deals with a scenario where the cyber attack adversely impacts the physical security digital assets used by the licensee to prevent unauthorized removal of material or radiological sabotage. Security digital assets include those used for nuclear material control and accounting.
(b) ~~The licensee shall~~To protect digital computer and communication systems and networks associated with the functions ~~listed~~described in ~~[§ 73.54~~paragraphs (a)(1~~)] in a manner that is commensurate with~~) and (2), the licensee shall: (1) Analyze the potential consequences resulting from cyber attacks on digital computer and communication systems and networks and identify those assets that must be protected to satisfy paragraph (a) of this section. (2) Implement the cyber security program in accordance with paragraph (d) of this section.	The adjusted language implements a graded approach to cyber security to accommodate the wide range of reactor technologies to be assessed by the NRC. The intent of the requirement is for licensees to protect the functions and associated systems from cyber attacks that cause the consequences identified in paragraph (a) above (e.g., safety functions, security functions). The graded approach will be further explained as part of a new regulatory guidance development effort. The licensee should analyze and identify which specific digital assets within the scope of § 73.110.
(c) The licensee shall meet the confidentiality, integrity, and availability requirements in § 73.54(a)(2) for the systems and networks ~~covered by~~identified in paragraph (b)(1) of this section in a manner that is commensurate with the potential consequences resulting from cyber attacks.	This paragraph is developed from § 73.54(a)(2). The intent of the requirement is to address the impacts on systems and networks (i.e., a compromise in confidentiality, integrity, or availability) from cyber attacks that need to be prevented. The adjusted language implements a graded approach to cyber security to accommodate the wide range of reactor technologies to be assessed by the NRC. The graded approach will be further explained as part of a new regulatory guidance development effort.
~~(d) The licensee shall:~~ ~~(1) Analyze the potential consequences resulting from cyber attacks on digital computer and communication systems and networks and~~	Requirements have been streamlined to merge paragraph (d) into paragraphs (b)(1) and (2).

~~identify those assets that must be protected to satisfy paragraphs (a), (b) and (c) of this section; and,~~ ~~(2) Establish, implement, and maintain a cyber security program for the protection of the assets identified under paragraph (d)(1) of this section.~~	
(~~e~~d) The cyber security program must be designed in a manner that is commensurate with the potential consequences resulting from cyber attacks through the following steps: (1) Implement security controls to protect the assets identified under paragraph (~~d~~b)(1) of this section from cyber attacks, commensurate with their safety and security significance; (2) Apply and maintain defense-in-depth protective strategies to ensure the capability to detect, delay, respond to, and recover from cyber attacks capable of causing the consequences identified in paragraph (a) of this section; (3) Mitigate the adverse effects of cyber attacks capable of causing the consequences identified in paragraph (a) of this section; and (4) Ensure that the functions of protected assets identified under paragraph (~~d~~b)(1) of this section are not adversely impacted due to cyber attacks ~~capable of causing the consequences identified in paragraph (a) of this section.~~ .	This paragraph is developed from § 73.54(c). The adjusted language implements a graded approach to cyber security to accommodate the wide range of reactor technologies to be assessed by the NRC. The graded approach will be further explained as part of a new regulatory guidance development effort. The overall intent of this requirement is to address the need for the licensee to develop a cyber security program that implements a defense-in-depth protective strategy. A defense-in-depth protective strategy for cyber security is represented by collections of complementary and redundant security controls that establish multiple layers of protection to safeguard critical digital assets. Under a defense-in-depth protective strategy, the failure of a single protective strategy or security control should not result in the compromise of safety and security functions.

(~~f~~e) The licensee shall implement the following requirements in a manner that is commensurate with the potential consequences resulting from cyber attacks:	This paragraph is developed from §§ 73.54(d) through 73.54(h). The adjusted language implements a graded approach to cyber security to accommodate the wide range of reactor technologies to be assessed by the NRC. The graded approach will be further explained as part of a new regulatory guidance development effort.
(1) As part of the cyber security program, the licensee ~~shall~~must meet the requirements in §§ 73.54(d)(1), 73.54(d)(2), 73.54(d)(4), and ~~the following:~~ ~~(i) Ensure~~must ensure that modifications to assets, identified under paragraph (~~d~~b)(1) of this section, are evaluated before implementation to ensure that the cyber security performance objectives identified in paragraph (a) of this section are maintained. (2) The licensee ~~shall~~must establish, implement, and maintain a cyber security plan that implements the cyber security program requirements of this section in accordance with the requirements ~~in § 73.54(e).~~ of this section. (i) The cyber security plan must describe how the requirements of this section will be implemented and must account for the site-specific conditions that affect implementation. (ii) The cyber security plan must include measures for incident response and recovery for cyber attacks. The cyber security plan must describe how the licensee will: (A) Maintain the capability for timely detection and response to cyber attacks; (B) Mitigate the consequences of cyber attacks;	The requirement is primarily intended to address the implementation of a cyber security program and the associated security life cycle activities for maintaining it such as continuous monitoring and assessment, configuration management, ongoing assessment of security controls and programs effectiveness, vulnerability scans/assessments, and cyber security event notifications. Potential conforming changes to § 73.77, "Cyber security event notifications," are under consideration by the NRC staff.

(C) Correct exploited vulnerabilities; and (D) Restore affected systems, networks, and/or equipment affected by cyber attacks. (3) The licensee shall develop and maintain written policies and implementing procedures to implement the cyber security plan ~~in accordance with the requirements in § 73.54(f).~~ . Policies, implementing procedures, site-specific analysis, and other supporting technical information used by the licensee need not be submitted for Commission review and approval as part of the cyber security plan but are subject to inspection by NRC staff on a periodic basis. (4) The licensee shall review the cyber security program in accordance with the requirements in § 73.100(~~e).~~ f). (5) The licensee shall retain all records and supporting technical documentation required to satisfy the requirements ~~in § 73.54(h).~~ of this section as a record until the Commission terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified by the Commission.	Pointer replaced with requirement from § 73.54(f). Pointer replaced with requirement from § 73.54(h).