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.

STAFF DISCUSSION OF PART 73 CYBER SECURITY – PRELIMINARY RULE LANGUAGE (June 2021)

Preliminary Language	Discussion
CYBER SECURITY	
§ 73.110 - Technology neutral requirements for protection of digital computer and communication systems and networks	In lieu of requiring advanced reactor licensees to protect against cyber attacks up to and including the design basis threat as required for power reactors in 10 CFR 73.54, this proposed new section implements a graded approach to determine the level of cyber security protection required for digital computer and 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 advanced reactor technologies. Specifically, the proposed new section requires licensees to demonstrate reasonable assurance of cyber security protection against cyber attacks only if the potential consequences from such attacks meet or exceed the consequences defined herein. The graded approach will be further explained as part of a new regulatory guidance development effort.

	The proposed new section leverages the following: (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 for advanced reactors as discussed above to accommodate the wide range of technologies to be assessed by the NRC.
(a) Each licensee 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 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 for advanced reactors to accommodate the wide range of technologies to be assessed by the NRC. Specifically, this section provides criteria for implementing a consequence-based approach to cyber security by determining whether the potential consequences resulting from a cyber attack would lead to the consequences listed herein. **The staff is interested in stakeholder views on whether any additional consequences should be included herein.**
(1) Exceeding the criterion in § 53.830(a)(2)(i);	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 the first tier safety criteria, as specified in § 53.830(a)(2)(i)).
(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 is intended to address the physical security requirements specified in § 53.830(a)(1). This consequence deals with a scenario where the cyber attack adversely impacts the digital assets used by the licensee to prevent unauthorized removal of special nuclear material, source material, and byproduct

	material (i.e., for protection of material SNM Cat III and Cat II (SSNM Cat I, if applicable) and Cat 1 and Cat 2 material.) Security digital assets include those used for nuclear material control and accounting.
(b) The licensee shall protect digital computer and communication systems and networks associated with the functions listed in [§ 73.54(a)(1)] in a manner that is commensurate with the potential consequences resulting from cyber attacks.	This paragraph is developed from § 73.54(a)(1). The intent of the requirement is to identify the types of systems and the functions that they support (e.g., safety functions, security functions, and emergency preparedness functions) that need to be protected from cyber attacks. This paragraph may not ultimately point to § 73.54(a)(1), as the Part 53 Working Group is going to have new definitions for certain functions and eliminate older definitions. For example, import-to-safety will not be used in Part 53, so this paragraph will need to be edited to capture the new terminology for what used to be called the "SSEP" functions. The adjusted language implements a graded approach to cyber security for advanced reactors to accommodate the wide range of technologies to be assessed by the NRC. The graded approach will be explained as part of a new regulatory guidance development effort.
(c) The licensee shall meet the confidentiality, integrity, and availability requirements in § 73.54(a)(2) for the systems and networks covered by paragraph (b) 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 for advanced reactors to accommodate the wide range of technologies to be assessed by the NRC. The graded approach will be 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 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.	This paragraph implements a graded approach to cyber security for advanced reactors to accommodate the wide range of technologies to be assessed by the NRC. The graded approach will be explained as part of a new regulatory guidance development effort. The licensee should analyze and identify which specific digital assets are actually critical digital assets, and thus within the scope of § 73.110. (Note: A 'critical digital asset' is a component of a critical system that consists of or contains a digital device, computer, or communication system or network.) Subsequently, the licensee shall establish, implement, and maintain a cyber security program for protecting those critical digital assets that makes use of risk insights, including threat information, and considers the resulting level of consequences of the threats.

(e) 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)(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)(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 for advanced reactors to accommodate the wide range of technologies to be assessed by the NRC. The graded approach will be 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 defensive strategy. A defense-in-depth defensive 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 defensive strategy, the failure of a single protective strategy or security control should not result in the compromise of safety and security functions.

(f) The licensee shall implement the following requirements in a manner that is commensurate with the potential consequences resulting from cyber attacks: (1) As part of the cyber security program, the licensee shall meet the requirements in §§ 73.54(d)(1), 73.54(d)(2), 73.54(d)(4), and the following: (i) Ensure that modifications to assets, identified under paragraph (d)(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 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). (3) The licensee shall develop and maintain written policies and procedures to implement the cyber security plan in accordance with the requirements in § 73.54(f). (4) The licensee shall review the cyber security program in accordance with the requirements in § 73.100(e). (5) The licensee shall retain all records and supporting technical documentation required to satisfy the requirements in § 73.54(h).	This paragraph is developed from §§ 73.54(d) through 73.54(h). The adjusted language implements a graded approach to cyber security for advanced reactors to accommodate the wide range of technologies to be assessed by the NRC. The graded approach will be explained as part of a new regulatory guidance development effort. 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.