NEI Comments on Cyber Security Draft Regulatory Basis

Section	Comment	Basis/Proposed Resolution
1. General	The regulatory basis includes an exemption for classified systems accredited by other agencies. If protections for SNM and classified information can be managed by other agencies, then these agency's protections for unclassified assets should also be acceptable. Dual regulation should be avoided which is a compliance challenge and a wasteful situation with no incremental increase in safety or security.	Include the following exemption for the application of this regulation: "Any digital asset residing within an accreditation boundary Certified and Accredited under another federal agency's (e.g., DOE, NNSA) cyber protection requirements is considered adequately protected and is exempt from the requirements of this regulation regardless of its function (e.g., physical security, MC&A)."
2. General	The list of digital assets that perform functions that could result in consequences of concern are well understood and analyzed in the ISA. The NRC should start with this subset of licensee digital assets to define the digital assets that should be within the scope of the rulemaking, rather than requiring the licensee to tabulate thousands of SSEPMCA digital assets for which no critical safety or security function has been identified.	Use plain language and clearly right size the scope of digital assets that would require protections under this rulemaking.
3. General	When performing the Risk Assessment to design appropriate cyber protections under this regulation, licensees should be able to consider the fact that failure mechanisms for cyber assets are already analyzed and mitigated with respect to failure effects in safety (ISA) and security (DBT and VA).	Provide clear direction in the rule for licensees to follow when performing risk assessments that allow them to utilize completed analyses for efficiency.
4. General	It is unnecessary to include emergency preparedness (EP) functions within the scope of this cyber security rulemaking.	EP plans are addressed in NRC approved, site-specific facility plans that contain redundancy in functionality. NRC and industry have agreed on this issue in reactor cyber security; crediting redundancy in systems in lieu of cyber security

Section	Comment	Basis/Proposed Resolution
		requirements.
5. General	It is unnecessary to include material control and accountability (MC&A) functions for Category III licensees with the scope of this cyber security rulemaking.	As stated by NRC during cyber security visits, MC&A security controls should be considered out of scope for Cat III's. The contention that some licensees use the MC&A management system in their ISA/ORPFS schemes should not be the basis for inclusion of all MC&A digital assets. The criteria that focuses on the consequences of concern to the public, worker, or environment will determine if a digital asset needs appropriate protection.
6. General	The draft Regulatory Basis for fuel cycle facilities contains no performance objective. The industry, in earlier discussions with the staff and in written comments, suggested consequences of concern to the public, worker, or environment establishing such performance objectives that would more clearly identify for each licensee those components and systems that need to be afforded protection and the appropriate level of protection. The final regulatory basis should adopt these suggested consequences of concern as performance objectives.	Without a performance objective that is specifically-tailored to the types of vulnerabilities that might be faced by a class of licensees, it is extremely difficult, if not impossible, for licensees to identify the digital assets that should be protected or to ensure appropriate protective measures are in place. In the absence of a clear performance objective, an overly-broad approach that does not consider vulnerabilities and consequences does not appear to be the most effective and efficient solution or use of our mutual resources including implementation and inspection.
7. Ch. 1, Pg 1-1	The draft regulatory basis would require that Category I licensees implement a cyber security programs that provides "high assurance" and Category II, III, and Part 40 licensees implement a program that provides "reasonable assurance". These terms are undefined in the document. Regardless of which term is used, the final regulatory basis should establish specific regulatory criteria for term used for each program.	Without context-specific criteria, the terms "high" and "reasonable" assurance lack distinct meanings. The Commission has explained that these terms have "comparable" meanings, which ultimately are determined by the "gravity" of the relevant concern. *See* 44 Fed. Reg. 68,185 (Nov. 28, 1979).

Section	Comment	Basis/Proposed Resolution
8. Ch. 1, Pg 1-1	Part 6 of the current definition of a cyber attack contains language that indicates that any adverse effect or consequence to a digital asset requires protection. There is no mention of consequences to safety or security. Furthermore, in many places, (pages 3-8, 3-9, 3-10, 4-2, 4-3, 4-4, 4-5, 4-6, etc.) the NRC draft regulatory basis document refers to a potential consequence of concern from a cyber-attack as loss of functionality.	Rulemaking should only address digital assets that result in a safety or security consequence to the public, worker, or environment. The definition and scope of rulemaking should be modified to reflect that. A lesson learned from the power reactor cyber security rule is to use a clearly defined concern based on a defined performance standard or objective rather than focusing on solely protecting the digital asset from compromise. Due to a variety of additional safety controls or the availability of alternate methods, loss of functionality of a digital asset needed for compliance does not automatically cause a consequence of concern. In most cases, loss of functionality is only a limiting condition of operation and safe shutdown or augmented compensatory action can be immediately taken.
9. Ch. 1, Pg 1-1	The objective to "codify in regulations the voluntary cyber security actions instituted by FCF licensees" can send the wrong signal to licensees and discourage self-identified and initiated future activities.	Proposed regulations need a regulatory basis/justification for the protection of the public, worker and environment, not to codify voluntary actions.
10. Ch 2.; Sec 2.1.5, Pg 2-3	The last paragraph sites a non-public report that NRC uses to assess the need for cyber security at fuel cycle facility licensees. This report should be provided to industry stakeholders that have security clearances and a need to know.	NRC should provide this report to industry to understand the assessment that determined rulemaking is required. *See Connecticut Light & Power Co. v. NRC*, 673 F.2d 525, 530-31 (D.C. Cir. 1982) ("An agency commits serious procedural error when it fails to reveal portions of the technical basis for a proposed rule in time to allow for meaningful commentary.").

Section	Comment	Basis/Proposed Resolution
11. Ch 2.; Sec 2.1.5, Pg 2-3	Section 2.1.5, page 2-3. Second paragraph, "the (NRC) working group determined that guidance used during development of the power reactor cyber security requirements, specifically NIST Special Publication 800-53…was appropriate for evaluating cyber security for fuel cycle facilities". Similar statement in Section 4.3, page 4-4, second paragraph," The proposed rulemaking will consider using nationally recognized and consensus standards (e.g. NIST SP 800-53, Rev 4) when addressing the protection of SSEPMCA functions." However, other cyber security guidance documents may be more appropriate for FCF facilities than NIST 800-53 (e.g., NIST SP 800-82 "Industrial Control System Security", ISO/IEC 27001 "International Organization for Standardization (ISO) Information Technology Security Techniques", ISO/IEC 21827 "System Security Engineering Capability" and ISA/IEC-62443 (formerly ANSI/ISA-99), "Procedures for Implementing Electronically Secure Industrial Automation and Control Systems (IACS)").	In SECY-12-0088, NRC recognized that "there are a wide variety of potential vulnerabilities and consequences resulting from a cyber-attack and that "not all FCFs are the same and that not all digital assets will require the same level of protection." In contrast, the staff's proposed use of a single NIST document appears to utilize a generic, one-size-fits-all approach that will result in an overly-broad application of cyber security controls that is not informed by the actual operational risks or consequences from a cyber-attack. NIST 800-53 was specifically designed for Security and Privacy Controls for Federal Information Systems and Organizations and it may be possible to apply some of these concepts to other types of systems and facilities. However, imposing this framework on all fuel cycle facilities without an actual evaluation of facility vulnerabilities and risk profile is impractical.
12. Ch. 3, Sec 3.3, Pg 3-7	Second paragraph: "the voluntary actions are not based on formal standards (e.g. NIST standards) and have been implemented in a manner that results in an ad hoc approach to the application of cyber security controls." This statement is not accurate. Contrary to this statement in the draft regulatory basis, the fuel-cycle industry used ISA/IEC standards, ISO based corporate policies, DOE orders, or CNSS instructions to implement the voluntary cyber security initiatives. This allowed licensees to use standards to meet their identified performance objectives.	To be accurate, the statement should be revised to as follows: "Industry voluntary cyber security control actions have been and continue to be implemented for a variety of reasons including safety, compliance, business continuity, protection of company sensitive or classified information, etc. These voluntary initiatives were developed using formal standards such as ISA/IEC standards, ISO based corporate policies, DOE orders, and CNSS instructions."

Section	Comment	Basis/Proposed Resolution
13. Ch. 4, Sec 4.3, Pg 4-3	First full paragraph: "in considering digital assets associated with safety, a licensee may utilize its ISA. However, the scope of the digital assets that may require…protection could extend beyond those identified with the aid of the ISA. 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."	Current NRC-approved ISA methodologies do not require consideration of malicious acts, these "additional analyses" will likely cause an ISA-type review and create a significant burden on licensees. Even if these additional analyses are kept separate from the existing facility ISA, licensees could conceivably be required to maintain two separate inspectable records (the current facility ISA and a new digital asset ISA considering malicious acts).
14. Ch. 4, Sec 4.4, Pg 4-5	The Table on Page 4-5, lists functions and their associated digital assets that require cyber protection. Many of these assets, MC&A, EP, and security are listed for cyber protection to "meet commitments." Digital assets should only require protection based on a safety or security consequence.	This rulemaking should only apply to assets that are needed to prevent a direct consequence to safety and security. This rule should not extend to items related for regulatory compliance alone. Revise the draft Regulatory Basis to remove any references to protection for compliance.
15. Ch. 4, Sec 4.5, Pg 4-7	The statement that the "rulemaking will provide additional assurance of a licensee's capability to protect their facility against a cyber attack" is a broad statement that has not been substantiated in the draft regulatory basis.	Provide quantitative information or analysis in the regulatory basis to justification this broad statement. This is another example of the focus on the cyber attack at the consequence of concern.
16. Ch. 5, Sec 5.2.2, Pg 5-3	This section implies that because NEI and industry endorsed a rulemaking to address the potential need for new cyber-security requirements for fuel-cycle facilities, they also endorsed the content or scope of the draft regulatory basis. NEI's 2013 letter expressed a preference for rulemaking as opposed to orders.	NEI's preference for rulemaking, as opposed to orders, is due to the open and transparent process that allows for stakeholder interaction where NRC provides a justification on the regulatory basis for a rule. We suggest that you remove all paragraphs from Section 5.2.2 except for the first one.
17. Ch. 8, Sec 8.6, Pg 8-4	First paragraph, "The NRC concludes that the costs associated with a cyber-security rulemaking will be offset by preventing cyber-attacks…"	This is an extremely weak cost justification implying that whatever the cyber rulemaking licensee cost, the safety and compliance benefits are worth it. First, there are no obvious safety or compliance

Section	Comment	Basis/Proposed Resolution
		benefits with protecting the functionality of certain SSEPMCA digital assets. Second, there is no support for the claim that a cyber-security program is "necessary to ensure FCF licensees provide adequate protection to the health and safety of the public and are in accord with the common defense and security."
18. Ch. 10, Sec 10.1, Pg 10-1	The statement "The RG will describe how these facilities should implement a cyber security program to protect systems and digital assets associated with safety, security (physical and information), emergency preparedness, and MC&A from cyber attacks." again demonstrates this Basis document with a mixed if not misplaced focus and objectives.	Correct the focus to be on the protection of the public, worker and environment.