Comments and NRC Staff Responses on the Draft Regulatory Basis for the Fuel Cycle Cyber Security Proposed Rulemaking

The NRC staff published a draft Regulatory Basis for comment on September 4, 2015, in the *Federal Register* (80 FR 53478). The NRC staff received nine separate comment letters (captured in Appendix A, "Table of Comments," of this document) prior to the comment period closing on October 5, 2015. The comment letters were evaluated and separated into 27 individual issues. Comments of a similar nature were grouped and summarized below. The NRC staff's disposition of the comments are also provided below.

Table of Contents

ISSUE 1. DUAL REGULATIONS 1
ISSUE 2. ESTABLISHING APPROPRIATE SCOPE 2
ISSUE 3. USE OF ISA 3
ISSUE 4. EMERGENCY PREPAREDNESS 4
ISSUE 5. EXCLUDE MATERIAL CONTROL AND ACCOUNTING 5
ISSUE 6. ESTABLISH CLEAR PERFORMANCE OBJECTIVES 6
ISSUE 7. DEFINE REASONABLE AND HIGH ASSURANCE 7
ISSUE 8. PREVENT CONSEQUENCES OF CONCERN 8
ISSUE 9. REMOVE THE OBJECTIVE TO CODIFY VOLUNTARY EFFORTS 9
ISSUE 10. RELEASE NON-PUBLIC REPORT 10
ISSUE 11. ALLOW INDUSTRY TO USE STANDARDS BEYOND NIST-800 SERIES 11
ISSUE 12. REVISE THE DESCRIPTION OF THE VOLUNTARY EFFORTS 12
ISSUE 13. MALICIOUS ACTOR ANALYSIS 13
ISSUE 14. JUSTIFY RULEMAKING 14
ISSUE 15. INDUSTRY SUPPORT FOR RULEMAKING OVER ORDERS 15
ISSUE 16. IMPROVED COST JUSTIFICATION 16
ISSUE 17. GRADED, RISK-INFORMED, AND PERFORMANCE-BASED 17
ISSUE 18. CONSISTENCY BETWEEN CYBER SECURITY AND PHYSICAL SECURITY 18
ISSUE 19. IMPLEMENT LESSONS LEARNED FROM REACTOR CYBER SECURITY 19
ISSUE 20. IMPLEMENT CONSISTENT REPORTING REQUIREMENTS 20
ISSUE 21. JUSTIFICATION FOR APPLYING THE PROPOSED RULE TO 10 CFR PART 40 FUEL CYCLE FACILITIES 21
ISSUE 22. PUBLISH PROPOSED GUIDANCE WITH PROPOSED RULEMAKING 22
ISSUE 23. APPLICABILITY OF BACKFIT 23
ISSUE 24. RISK ASSESSMENT 24
ISSUE 25. USE OF NIST STANDARDS 25
ISSUE 26. THE NRC SHOULD STOP WORK ON A NUMBER OF REGULATORY ACTIVITIES 26
ISSUE 27. VULNERABILITY MOTIVATING RULEMAKING 27

ISSUE 1. DUAL REGULATIONS

NRC-Designated Comment Numbers: 1.11, 2.1, 3.3, 3.21, 4.14, and 8.1

Comment Summary:
Several commenters indicated that dual regulation would make compliance challenging and unnecessarily waste resources. The NRC should allow licensees to exempt digital assets that are certified or accredited under another Federal agency's (e.g., U.S. Department of Energy (DOE), National Nuclear Security Administration (NNSA)) cyber protection requirements. If special nuclear material (SNM), classified information, or business networks are regulated by other Federal agencies, the NRC should exempt these systems from the proposed NRC regulations.

NRC's Position:
The NRC Fuel Cycle Cyber Security Working Group (staff) agrees in principle that dual regulation should be avoided where possible. The NRC staff is considering approaches whereby licensees could take credit for compliance with equivalent requirements from other regulatory authorities. Approaches under consideration include guidance that describes an acceptable approach to credit existing equivalent cyber protections to demonstrate compliance with proposed cyber security regulations; allowing the use of an exemption from NRC regulations, provided the exemption can be justified; etc.

Response Summary:
The regulatory basis (RB) has been revised in Section 3.3 to state that the goal of the proposed NRC FCF cyber security rulemaking is to allow licensees to take credit for compliance with cyber security requirements of another federal agency that provides a level of protection at least equivalent to the requirements in the rule. If the licensee analysis documents an equivalent level of protection, the licensee will not need to apply the relevant controls required by the rule.

ISSUE 2. ESTABLISHING APPROPRIATE SCOPE

NRC-Designated Comment Numbers: 1.5, 1.8, 2.2, 2.18, 3.2, 3.9, 4.11, 7.5, 8.2, 8.3, 10.1, 10.2, 10.10, 11.1, 11.2, and 11.6

Comment Summary:
Several commenters indicated that the scope of the proposed rulemaking should be refined. The commenters expressed concern that digital assets used for business purposes should be excluded from consideration in the rulemaking. Licensees should only be required to analyze digital assets whose compromise could result in a consequence of concern. The scope of the analysis should be limited in order to prevent licensees from evaluating thousands of digital assets, most of which would be screened out as not requiring cyber security controls. One commenter indicated that the degradation of items relied on for safety (IROFS) should not be considered a consequence of concern.

NRC's Position:
The NRC staff agrees that the scope of the proposed rulemaking should be to protect those digital assets related to safety, security, and safeguards (3S) functions that, if compromised, could result in a consequence of concern. Digital assets outside of these areas, such as those relied on solely for business purposes, would be excluded from the scope of the rule. The NRC staff anticipates that controls would only be required for digital assets associated with, or whose compromise could result in, a consequence of concern. Accordingly, the NRC staff expects that the proposed rulemaking would require protection of IROFS only in cases where a cyber attack compromising the function of the IROFS results in a consequence of concern.

Response Summary:
The RB has been revised in Section 4.4 to clarify that licensees may use existing safety analyses (e.g., integrated safety analysis (ISA), security plan) to inform the analysis of digital assets and reduce the regulatory burden. However, some additional analysis would be required to address malicious acts (i.e., cyber attacks), which may not have been previously analyzed. The RB has been modified throughout to state that only digital assets associated with, or whose compromise could result in, a consequence of concern would need to be protected. The draft consequences of concerns, associated thresholds, and conceptual screening methodology are provided in the RB, Section 4.4.

ISSUE 3. USE OF ISA

NRC-Designated Comment Numbers: 2.3, 4.2, 7.3, 7.5, 7.7, 7.8, 7.13, 7.16, 7.18, and 11.7

Comment Summary:
Multiple commenters indicated the NRC should allow licensees to take into consideration that failure mechanisms for cyber assets may already be analyzed and mitigated with respect to safety and security via the ISA and other existing programs. The NRC should also allow licensees to use existing knowledge and hazard information from the ISA and security programs to inform the risk assessment and analyses to identify digital assets associated with a consequences of concern.

NRC's Position:
The NRC staff agrees that existing analyses should be utilized by licensees to limit the regulatory burden of identifying digital assets whose compromise could result in a consequence of concern. However, the NRC staff believes that additional analysis may be needed to address malicious acts. The additional analysis would not require changes to licensees' existing analyses. The NRC staff encourages licensees to use existing knowledge and hazard information from the ISA and security programs to inform the risk assessment and analyses to identify digital assets associated with a consequence of concern.

Response Summary:
Additional text has been added to the RB in Section 4.3 to clarify that a compromise of a digital asset may involve a malicious act that typically has not been evaluated in the licensees' existing safety analyses. Therefore, additional analyses to address the malicious aspects may need to be conducted for all digital assets that could result in a consequence of concern. Existing language on this topic remains in the RB in Sections 2.2.2 and 3.3. The NRC staff anticipates that use of existing safety and security programs would reduce the regulatory burden of evaluating digital assets for cyber security.

ISSUE 4. EMERGENCY PREPAREDNESS

NRC-Designated Comment Number: 2.3 and 11.5

Comment Summary:
One commenter suggested that the proposed rulemaking should exclude emergency preparedness (EP) functions from the scope of the cyber security proposed rulemaking since these systems have significant redundancy and cannot result in a consequence of concern.

NRC's Position:
The NRC staff agrees that digital assets associated with EP do not result in a consequence of concern unless they also have a nexus to safety (e.g., emergency notification systems), in which case they would be evaluated under the safety category.

Response Summary:
The RB has been modified to state that EP functions only need to be considered in cases where they support (i.e., provide an input to) 3S functions associated with a consequence of concern. EP functions do not need to be addressed separately because the diversity of EP functions and capabilities provide non-digital redundancies (i.e., equivalent function by alternate means).

ISSUE 5. EXCLUDE MATERIAL CONTROL AND ACCOUNTING

NRC-Designated Comment Number: 2.5, 6.5, and 11.5

Comment Summary:
Several commenters indicated the NRC should not include material control and accounting (MC&A) systems within the scope of the proposed rulemaking for Category III facilities. Although one commenter recognized that the MC&A program may be used to support the ISA, the commenter did not agree that this was a sufficient basis to include all MC&A digital assets within the scope of the proposed rulemaking.

NRC's Position:
The NRC staff agrees that MC&A does not need to be explicitly included within the scope of the proposed rulemaking. MC&A systems that are used for safety or security programs would be evaluated within the scope of 3S functions.

Response Summary:
The RB has been revised (throughout) to remove MC&A from the scope of the proposed rulemaking for Category III licensees. However, the RB also indicates that MC&A functions must be evaluated in cases where they are relied upon to provide a safety (e.g., mass control) or safeguard function associated with a consequence of concern, particularly at Category I facilities. In these cases, digital assets associated with MC&A would be within the scope of the proposed rulemaking and addressed as part of the 3S functions.

ISSUE 6. ESTABLISH CLEAR PERFORMANCE OBJECTIVES

NRC-Designated Comment Numbers: 1.7, 2.6, 3.5, 3.12, 3.15, 3.16, 3.18, 3.22, 4.10, 4.17, 6.1, 6.2, 7.10, 10.4, 11.3, and 11.5

Comment Summary:
Multiple commenters expressed the need to establish clear performance objectives that are risk-informed. The commenters indicated the performance objectives should be tailored to the types of vulnerabilities possible for different classes of licensees. Several commenters suggested that the NRC should adopt the performance objectives provided by industry in the Nuclear Energy Institute's (NEI's) letter to the NRC dated October 2013, "Cyber Security Control Assessments, Rev. 2" (ADAMS No. ML14351A288) or explain why these proposals are not applicable. Another commenter proposed that the performance objectives be based on 10 CFR 70.61. One commenter indicated licensees would have difficulty identifying the digital assets that must be protected without explicit performance objectives that are tailored based on facility type.

NRC's Position:
The NRC staff agrees that the RB should establish clear performance objectives. These would be based in part on the performance objectives in 10 CFR 70.61, in addition to security requirements (e.g., 10 CFR 73.1 – Design Basis Threat). The NRC has reviewed NEI's October 2013 letter and incorporated a number of proposals into the performance objectives including: addressing both active and latent consequences of concern, allowing licensees to take credit for an equivalent function performed through alternate means, allowing licensees to apply common controls to a set of similar digital assets, and implementing a screening criteria with similar intent to NEI's proposed consequence assessment. Although NEI's October 2013 letter has informed the NRC's regulatory approach, this approach continues to develop over time based on stakeholder feedback, lessons learned from the implementation of 10 CFR 73.54, staff insights, and other information.

Response Summary:
The RB has been revised (Chapter 1) to state that the proposed rule would require licensees to establish and maintain a cyber security program for the protection of digital computer systems, communication systems, and networks associated with 3S functions from cyber attacks that could result in a consequence of concern. Meeting this primary performance objective is accomplished by applying controls to digital assets that perform 3S functions. The consequences of concern are summarized in Chapter 1 of the RB and additional description has been added to the table in Section 4.4 of the RB that identifies the types of events to be protected against.

ISSUE 7. DEFINE REASONABLE AND HIGH ASSURANCE

NRC-Designated Comment Number: 2.7 and 3.7

Comment Summary:
One commenter stated that the RB does not differentiate between the high assurance proposed for Category 1 facilities and reasonable assurance proposed for other facilities. The commenter indicated that high assurance has been used by the Commission for postulated accidents related to sabotage of power reactors. This level of assurance does not appear appropriate for Category I licensees. The NRC staff should provide context-specific criteria to allow licensees to better determine the comparable meaning of high and reasonable assurance as applied to fuel cycle facilities.

NRC's Position:
The NRC staff agrees that high and reasonable assurance involves a technical evaluation that depends on the system under consideration. The NRC staff plans to include examples of the type of information needed for each category of licensee to demonstrate compliance with the performance objectives in the guidance for the proposed rulemaking.

For the purposes of this rulemaking, the level of protection is provided by cyber security controls, defense-in-depth, and supporting systems, structures, and programs put in place to assure that in-scope, digital assets remain available and reliable. The NRC staff envisions that digital assets associated with the DBT would require an increased number and robustness of cyber security controls compared to non-DBT digital assets.

Response Summary:
The RB (Chapter 1 and 4) indicates that the proposed 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 program is graded to provide assurance of adequate protection based on the level of SNM processed at these facilities. The Category I facilities would be required to implement additional baseline controls for digital assets utilized to meet the DBT requirements.

ISSUE 8. PREVENT CONSEQUENCES OF CONCERN

NRC-Designated Comment Numbers: 2.8, 2.14, 2.18, 4.6, 6.3, 6.4, and 7.8

Comment Summary:
Multiple commenters indicated that the focus of the cyber security rulemaking should be to prevent a consequence of concern to workers, the public, or the environment, rather than ensure regulatory compliance, preserve system functionality, or protect digital assets. Several commenters noted that a loss of functionality to a digital asset may not necessarily result in a consequence of concern. One commenter stated that digital assets associated with MC&A and EP involve compliance and would not result in a consequence of concern. One commenter indicated that the NRC should require each licensee to perform a vulnerability assessment to determine if digital assets could result in a consequence of concern.

NRC's Position:
The NRC staff agrees that the focus of the proposed rulemaking should be to protect those digital assets related to 3S functions that, if compromised, could result in a consequence of concern. To accomplish this, the proposed rule would require licensees to apply controls to those digital assets whose compromise could result in a consequence of concern.

The NRC staff agrees that the compromise of digital assets associated with MC&A and EP do not result in a consequence of concern, unless there is a nexus to safety or security (e.g., mass control to protect against criticality). Therefore, the scope of the proposed rulemaking has been modified to address only those MC&A and EP assets that impact the 3S functions. The NRC staff agrees that the proposed rule language should include a requirement for licensees to identify digital assets that could result in a consequence of concern. The RB has been revised to identify the consequences of concern that are expected to be the focus of the proposed rulemaking.

Response Summary:
The revised RB states that the performance objective is to protect facilities against a cyber attack associated with a consequence of concern. The definitions of active and latent consequences of concern have been added and the related thresholds for each consequence of concern are provided. The RB has been revised (throughout) to reflect that EP functions only need to be considered in cases where they support (i.e., provide an input to) 3S functions associated with a consequence of concern. The RB indicates in Section 4.4 and throughout that an assessment would be required to evaluate digital assets associated with 3S functions. This analysis would determine if a compromise of the digital asset could result in an active or latent consequence of concern either through failure or compromise of the asset's function (i.e., cease functioning or function in a malicious manner).

ISSUE 9. REMOVE THE OBJECTIVE TO CODIFY VOLUNTARY EFFORTS

NRC-Designated Comment Number: 2.9

Comment Summary:
One commenter stated that the RB should not include the objective to "codify" the voluntary cyber security actions implemented by fuel cycle facilities. This objective would discourage future self-identification of voluntary cyber security initiatives. In addition, there is insufficient basis for incorporating the voluntary initiatives into the regulations.

NRC's Position:
The NRC staff agrees with the comment.

Response Summary:
The objective to "codify" voluntary cyber security actions has been removed from the RB.

ISSUE 10. RELEASE NON-PUBLIC REPORT

NRC-Designated Comment Number: 2.10

Comment Summary: One commenter stated the NRC should make available a non-public report relied on to justify the need for the proposed rulemaking to industry stakeholders with appropriate clearances. This information is needed to fully understand the basis for the rulemaking.

NRC's Position:
The NRC staff agrees in part, as much information as is feasible for release to industry should be made available to inform stakeholders regarding the basis for the proposed rulemaking. However, certain security, proprietary, and internal – official use only information cannot be released due to the potential vulnerabilities and licensee specific trade secrets discussed within.

Response Summary:
The RB has been revised in Section 2.1.5 to incorporate a brief summary of the conclusion from the non-public working group report, February 25, 2012, "U.S. Nuclear Regulatory Commission Cyber Security for Fuel Cycle Facilities Working Group Final Report." The reference to the non-public document has been retained in the RB for NRC use.

ISSUE 11. ALLOW INDUSTRY TO USE STANDARDS BEYOND NIST-800 SERIES

NRC-Designated Comment Numbers: 2.11, 6.6, 8.4, 10.1, and 10.3

Comment Summary:
Multiple commenters indicated the NRC should avoid requiring licensees to comply with a single set of industry standards (i.e., National Institute of Standards and Technology (NIST) Special Publication (SP) 800 series) in the guidance for the proposed rulemaking. The fuel cycle industry should be allowed to implement alternate standards (e.g., ISO/IEC 27001, "International Organization for Standardization (ISO) Information Technology Security Engineering Capability (IEC)," and ISA/IEC-62443 (formerly ANSI/ISA-99), "Procedures for Implementing Electronically Secure Industrial Automation and Control Systems (IACS)"), aspects of which may have already been implemented at certain fuel cycle facilities. The NRC should avoid implementing a generic, one-size-fits-all approach to the wide range of fuel cycle facilities and instead allow use of equivalent standards. One commenter supported the use of the NIST SP 800 series as the basis for an NRC cyber program.

NRC's Position:
The NRC staff agrees that a licensee should be allowed to utilize cyber security guidance documents other than the NIST standards as long as the licensee can demonstrate compliance with NRC regulatory requirements. The regulatory guidance accompanying the proposed rulemaking would provide one acceptable approach for meeting the requirements. The guidance would reference NIST standards as one acceptable approach for identifying controls and developing a cyber program. Alternate approaches based on equivalent standards are also acceptable, provided these standards provide an equivalent level of protection and the licensee demonstrates compliance with the regulations.

Response Summary:
Although the RB continues to refer to NIST standards as one approach acceptable to the NRC staff, revised text in Section 2.1.5 clarifies that nationally recognized standards (e.g., ISO/IEC 27000 series standards, DOE standards, and U.S. Department of Defense (DOD) standards) may also be acceptable, provided licensees demonstrate compliance with the final regulations. Existing language on this topic remains in the RB in Sections 4.3 and 4.7.

ISSUE 12. REVISE THE DESCRIPTION OF THE VOLUNTARY EFFORTS

NRC-Designated Comment Numbers: 2.12, 3.13, 3.14, 3.18, 5.2, 6.1, and 6.7

Comment Summary:
Several commenters indicated that the NRC should consider revising the description of industry's voluntary cyber security efforts. Licensees used a number of guidance documents to inform their implementation of voluntary efforts which are not recognized in the RB.

NRC's Position:
The NRC staff agrees that the voluntary efforts have been implemented differently across the fuel cycle industry for a variety of reasons, including safety, business applications, security, protection of information, etc. The NRC reviewed a number of licensee voluntary cyber security efforts in August through October of 2015 through interactions including document reviews, conference calls, and site visits (ADAMS No. ML15314A621). These site visits revealed a wide range of cyber security initiatives being implemented throughout the fuel cycle industry. Generally, the cyber security programs show improvement since the previous visits conducted in 2013, but the wide range of voluntary efforts allows for potential gaps in analyses, application of controls, and implementation of cyber security programs. The NRC staff also agrees that various facilities have used a range of industry standards, including NIST and ISO standards. The NRC continues to believe that the wide range of cyber security standards, programs, and controls implemented on a voluntary basis throughout the fuel cycle industry results in gaps in the protection of 3S functions which could lead to a consequence of concern.

Response Summary:
Chapter 2 of the RB provides information on industry voluntary efforts. As described in Section 2.1.6, NEI indicated in a July 3, 2013 letter (non-public ADAMS No. ML14174B231) that fuel cycle facility (FCF) licensees would independently consider four near-term voluntary actions which include:

1. establish a cyber security team (CST);
2. provide cyber security awareness training to staff;
3. establish a cyber security incident response capability; and
4. provide security controls that address portable media, devices, and equipment (PMDE).

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 do not fully address protection of safety, security, emergency preparedness, and material control and accounting functions. Section 2.1.6 of the RB states that, although industry has implemented voluntary actions, the actions lack a comprehensive analysis and, in certain cases, addressed only a limited number 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.

ISSUE 13. MALICIOUS ACTOR ANALYSIS

NRC-Designated Comment Numbers: 2.13 and 6.8

Comment Summary:
Multiple commenters stated that even though the existing analysis in the ISA can be used to inform the cyber security analysis, the existing program does not consider malicious acts on digital assets. Therefore, licensees would have to invest significant resources to evaluate these types of events. This effort would require an ISA type review conducted by a team of licensee staff with experience with the facility. This effort would have significant burden on the licensees.

NRC's Position:
The NRC staff agrees in part, the existing programs such as the ISA can be used to identify digital assets associated with 3S functions that could lead to a latent or active consequence of concern. The NRC staff also agrees that licensees would need to evaluate malicious acts (i.e., cyber attacks) that could result in latent or active consequences of concern, outside the scope of the existing ISA analysis. However, the NRC staff disagrees that the analysis would involve an expansion of the ISA analysis. The analysis would be conducted independent of the ISA as part of the cyber security program. The NRC staff recognizes that the additional analysis to identify and protect against cyber attacks would impose additional regulatory burden and associated costs. As currently envisioned, licensees would need to analyze digital assets associated with 3S functions and implement controls on assets whose compromise could result in a consequence of concern. Additional opportunities for stakeholder feedback on the potential costs will be provided to inform the proposed rulemaking and cost analysis.

Response Summary:
Text has been added to the RB in Section 4.3 to confirm that existing licensee programs such as the ISA can be used to identify digital assets that need to be protected against a consequence of concern. Section 4.3 of the RB has also been modified to recognize that additional analyses, beyond the scope of the ISA, would be needed to address cyber attacks. Section 8.2 of the RB also indicates that the burdens on licensed facilities include the following: (1) conducting an analysis to identify assets that would require additional cyber security measures; (2) establishing an NRC-approved cyber security program; (3) maintaining the cyber security program and configuration management program; and (4) documentation and event reporting regarding the cyber security program to the NRC.

ISSUE 14. JUSTIFY RULEMAKING

NRC-Designated Comment Number: 1.1, 1.4, 1.10, 2.15, 3.10, 4.1, 4.2, 4.5, 4.13, 10.6, and 7.21

Comment Summary:
Several commenters indicated that the RB does not justify rulemaking and additional information is needed to substantiate the NRC staff claim that the proposed rulemaking would provide additional assurance of the licensee's capability to protect their facility against a cyber attack. The proposed rulemaking should focus on protecting against a consequence of concern rather than a cyber attack. The RB should also justify the statement that a cyber program is needed to protect health and safety. Several commenters questioned the ability for cyber sabotage to result in new critical target areas.

NRC's Position:
The NRC staff disagrees that the RB does not justify the proposed rulemaking. The RB identifies a regulatory gap for existing cyber security regulations for fuel cycle facilities. The growing use of digital assets for licensee 3S functions produces a potential for the compromise of a function which could result in a consequence of concern. Industry's attempt to mitigate the regulatory gap through voluntary cyber security efforts have been varied and in several cases lack robustness. The NRC staff observed a number of areas for improvement at FCF licensees including a need for licensees to identify digital assets, analyze them for potential consequences of concern, implement necessary controls, and document that a sufficient program is in place to prevent a consequence of concern due to a cyber attack.

The NRC staff agrees that the goal of the proposed rulemaking should be to protect those digital assets related to 3S functions that, if compromised, could result in a consequence of concern. The NRC staff recognizes that preventing cyber attacks is not always within the control of the licensee. The proposed rulemaking would require licensees to identify and protect digital assets whose compromise may result in a consequence of concern, and would define thresholds for consequences of concern beyond the scope of the critical target area analysis. The proposed rulemaking would require licensees to develop and implement an NRC-approved cyber security program that provides assurance that controls are adequate to prevent a consequence of concern.

Response Summary:
Chapter 1 of the RB now states that the goal of the proposed rule is to require licensees 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 3S functions from cyber attacks that could result in a consequence of concern. Section 4.4 of the RB provides a table with draft thresholds for consequences of concern and an overview of digital assets that the NRC staff expects to consider when defining 3S functions. The NRC staff expects to develop regulatory guidance to identify acceptable control sets that licensees may implement to protect 3S functions from compromise that could result in a consequence of concern.

ISSUE 15. INDUSTRY SUPPORT FOR RULEMAKING OVER ORDERS

NRC-Designated Comment Number: 2.16

Comment Summary:
One commenter indicated that the RB reference to NEI's 2013 letter expressing a preference for rulemaking over orders should not be misconstrued to imply support for the agency's RB. The reference to NEI's letter should be removed in its entirety from the RB.

NRC's Position:
The NRC staff disagrees that the reference to NEI support for proposed rulemaking should be removed in its entirety from the RB. The reference illustrates that the industry recognizes the nexus cyber security has to safety and that a sound regulatory structure is warranted. The NRC staff agrees that the reference to the NEI letter supporting a proposed rulemaking should not be misconstrued as support for the NRC's RB.

Response Summary:
Section 5.2.2 of the RB has been revised to reduce the amount of text quoted from the NEI letter. The reduced quotation is designed to more accurately reflect NEI's recommendation that rulemaking is preferable to orders. The quotation also illustrates industry support for "protecting those digital assets whose compromise would directly challenge a licensee's operational safety and security, resulting in a consequence of concern."

ISSUE 16. IMPROVED COST JUSTIFICATION

NRC-Designated Comment Numbers: 1.13, 2.17, 3.6, 3.17, 3.23, 4.8, 6.9, 7.15, 7.17, 10.8, 11.8, and 11.9

Comment Summary:
Multiple commenters stated that the cost justification in the draft RB should be improved. The RB should justify the statement that the savings from preventing a consequence of concern from a cyber attack would exceed the cost of implementing a cyber program. The justification should take into consideration risk considerations. Several commenters indicated that the scope of the proposed rulemaking would impact the costs of implementation. If the proposed rule language requires all digital assets to be analyzed, the costs of implementation would be significant.

NRC's Position:
The NRC staff agrees in part and disagrees in part with the comments regarding cost. The NRC staff agrees that a comprehensive cost justification should be developed as part of the regulatory analysis in the *Federal Register* notice that accompanies the proposed rulemaking. However, the NRC staff disagrees that this same rigor should be developed in the RB. The NRC staff disagrees that the costs to implement cyber security cannot be justified and the RB discusses several considerations that the NRC would examine in developing the comprehensive cost justification.

Response Summary:
Chapter 8 of the RB clarifies that the NRC expects the costs of implementation to be justified based on providing protection from a cyber attack resulting in a consequence of concern. The performance objectives in the RB have been clarified as protection of digital assets whose compromise could result in a consequence of concern. This improved definition of the scope should further limit the estimated costs (i.e., fewer digital assets requiring cyber security controls). Stakeholders would have additional opportunity to comment on the in-depth cost estimates under development for the regulatory analysis during the comment period for the proposed rulemaking.

ISSUE 17. GRADED, RISK-INFORMED, AND PERFORMANCE-BASED

NRC-Designated Comment Number: 1.2, 4.3, and 7.6

Comment Summary:
Several commenters indicated the proposed rulemaking should be consistent with the NRC's historical risk-informed, and performance-based approach and framework for protection of SNM. The proposed rule should be graded based on the facility's risk profile. Grading of the requirements should not be implemented only in the guidance.

NRC's Position:
The NRC staff agrees in part. The NRC staff agrees that the proposed rulemaking should be graded, risk-informed, and performance-based. It is expected that the proposed rule would meet these criteria. The baseline set of cyber security controls is graded based on the facility type, for example fuel cycle facilities with Category I materials would have a "high" cyber security control baseline (i.e., control set) whereas a Category III facility may not require the application of any controls unless digital assets have a nexus to 3S functions. The evaluation of digital assets utilizes risk-informed concepts (i.e., consequences of concern and associated thresholds) and existing, risk-informed programs (i.e., ISA and physical security program) to support the identification of digital assets within the scope of the proposed rulemaking. The proposed rulemaking would be performance-based because licensees would retain significant flexibility in determining and implementing the mechanism to accomplish the rule's objectives. For example, licensees may decide to apply controls to digital assets or implement alternate means to perform an equivalent function.

Response Summary:
Section 4.4 of the RB has been revised to better describe graded, risk-informed, and performance-based aspects of the program, including the consequences of concern and the facility type approach. In particular, a table has been added to better define the thresholds envisioned for the consequences of concern that could result from a cyber attack and must be protected against.

ISSUE 18. CONSISTENCY BETWEEN CYBER SECURITY AND PHYSICAL SECURITY

NRC-Designated Comment Numbers: 1.3, 1.6, 3.1, 3.2, 3.4, 4.4, 4.9, and 11.4

Comment Summary:
Several commenters questioned the need to apply cyber security requirements equally across the diverse range of fuel cycle facilities even though the physical security requirements, risks, and types of material are diverse for the various types of facilities (i.e., source material, Category I, II, and III). Several commenters questioned the need to apply cyber security requirements to malicious actor events at all fuel facilities when physical security for malicious actors only applies to certain fuel cycle facilities.

NRC's Position:
The NRC staff disagrees that the RB applies cyber security requirements equally across the diverse range of FCFs. The revised RB states that cyber security requirements should be applied in a graded manner to different types of facilities. The NRC staff agrees that certain facility types require only a limited set of cyber security controls due to the limited, potential consequences of concern. Other types of facilities that have a DBT or significant sources of enriched SNM require a higher level of cyber security. The revised RB proposes a range of cyber security controls that can be applied on a facility type basis.

The NRC staff believes that cyber security regulations are justified, on a graded scale, for all fuel cycle facilities even when physical security requirements may not be warranted (e.g., source material facilities, certain category III facilities). This is due to the fundamental differences between a physical attack and a cyber attack as well as the potential consequences of concern at fuel cycle facilities.

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 digital systems or assets is potentially significantly higher for a cyber attack than for a physical attack. Because of these significant differences, the NRC staff believes that cyber security requirements should be applied on a graded scale, based on potential consequences of concern, to all fuel cycle facilities as an aspect of physical security considerations.

Response Summary:
Section 4.4 of the RB has been modified to clarify that a range of cyber security controls would be applied depending on the facility type. The new text also describes some of the differences between physical security and cyber security which supports establishing a different set of thresholds for cyber security than for physical security (Section 4.3). The new text also indicates that Category III facilities should have cyber security controls applied for physical security assets only when those assets have a nexus to safety or possess classified information/material.

ISSUE 19. IMPLEMENT LESSONS LEARNED FROM REACTOR CYBER SECURITY

NRC-Designated Comment Numbers: 3.19, 4.7, 7.11, and 7.14

Comment Summary:
Several commenters recommended the NRC take into consideration the lessons learned from the power reactor rulemaking to avoid pitfalls and undue burden to NRC and industry.

NRC's Position:
The NRC staff is incorporating lessons learned from the reactor cyber security rulemaking. The lessons learned include: scoping of digital asset/systems must be specific, establishing a screening process, providing clear safety and security objectives, ensuring licensee programs and processes are sound prior to focusing on technical implementation, switching the focus from implementation of specific cyber security controls to protecting against a potential consequence of concern, and establishing an implementation schedule with firm deadlines.

Response Summary:
Section 2.1.3 of the RB has been revised to include a list of the lessons learned from the power reactor cyber security rulemaking.

ISSUE 20. IMPLEMENT CONSISTENT REPORTING REQUIREMENTS

NRC-Designated Comment Number: 1.9, 3.13, and 4.12

Comment Summary:
Several commenters indicated the NRC should use existing reporting requirements to be notified of cyber security events, rather than develop new cyber security reporting requirements.

NRC's Position:
The NRC staff agrees that the cyber security reporting requirements should be consistent with existing reporting requirements; however, additional notification and documentation may be needed for cyber security events.

Response Summary:
Section 4.4 of the RB has been revised to state that wherever possible, the cyber security reporting requirements would be consistent with existing reporting requirements.

ISSUE 21. JUSTIFICATION FOR APPLYING THE PROPOSED RULE TO 10 CFR PART 40 FUEL CYCLE FACILITIES

NRC-Designated Comment Numbers: 1.12, 3.8, 4.15, 7.2, 7.4, 7.9, 7.11, and 7.12

Comment Summary:
Several commenters indicate that fuel cycle facilities licensed under 10 CFR Part 40 should be excluded from the proposed rulemaking because they do not have the same level of physical security requirements and vulnerabilities as fuel facilities that process SNM. One commenter indicated that chemical concerns are not addressed in the RB. Several commenters stated that the proposed rulemaking should allow for facility specific requirements tailored to the risks at each type of fuel cycle facility. As currently envisioned, the cyber security proposed regulations are focused on SNM and do not apply to the lower risks at a facility licensed under 10 CFR Part 40. The proposed rulemaking should allow enough flexibility to apply to different types of operations and risks at the different types of fuel cycle facilities.

NRC's Position:
The NRC staff agrees in part with the comment. The NRC staff agrees that the cyber security risks at a 10 CFR Part 40 fuel cycle facility are different than the risks at a 10 CFR Part 70 fuel cycle facility. Although the NRC staff agrees that 10 CFR Part 40 fuel cycle facilities do not have a DBT, the NRC staff disagrees with the implication that there are no consequences of concern that could result from a cyber attack. The performance objective of protecting against a consequence of concern and the application of controls based on the facility type both provide significant grading of the proposed requirements. Certain licensees (i.e., conversion and deconversion facilities) have the potential for significant chemical exposures and are required by NRC regulations and orders to meet specific operational safety requirements. This risk-informed approach, taking into account facility type grading, would ensure 10 CFR Part 40 facilities have the appropriate level of controls based on the facility risks.

Response Summary:
The RB has been revised in Sections 3.1 and 4.3 to describe why cyber security requirements are different than physical security requirements, including for conversion and deconversion facilities. Section 4.4 of the RB has been updated to identify the types of consequences of concern, associated thresholds, and conceptual screening methodology. These include considerations for a chemical release. In addition, the RB indicates throughout that the proposed requirements will incorporate flexibility through grading of the requirements based on facility type, including for conversion and deconversion facilities.

ISSUE 22. PUBLISH PROPOSED GUIDANCE WITH PROPOSED RULEMAKING

NRC-Designated Comment Number: 7.5

Comment Summary:
One commenter indicated the NRC staff should develop and publish proposed guidance concurrently with the proposed rulemaking. This would allow stakeholders to provide more informed comments on the proposed rule package.

NRC's Position:
The NRC staff agrees that the proposed guidance should be published at the same time as the proposed rulemaking. The *Federal Register* notice for the proposed rulemaking would reference the proposed guidance, which would be publicly available at that time.

Response Summary:
Section 4.4 of the RB has been revised to clarify that the NRC plans to publish the proposed guidance with the proposed rulemaking.

ISSUE 23. APPLICABILITY OF BACKFIT

NRC-Designated Comment Numbers: 1.13, 3.11, 3.11, 7.19, and 7.20

Comment Summary:
Several commenters suggested that the NRC conduct a backfit analysis for the proposed rulemaking. One commenter requested that the equivalent of a backfit analysis be conducted for 10 CFR Part 40 facilities.

NRC's Response:
The NRC staff agrees in part with the comment to conduct a backfit analysis. The NRC staff agrees that a backfit analysis is required for certain facilities licensed under 10 CFR Part 70. The backfit analysis for 10 CFR Part 70 facilities would be developed as part of the proposed rulemaking package. The NRC staff disagrees with the comment to conduct a backfit analysis for 10 CFR Part 40 facilities. The regulations in 10 CFR Part 40 do not contain backfit provisions so no backfit analysis would be conducted for facilities licensed under this part. However, the NRC staff notes that the regulatory analysis prepared for the proposed rulemaking would contain a cost benefit analysis for all facilities subject to the proposed rulemaking, including those licensed under 10 CFR Part 40.

Response Summary:
Chapter 6 of the RB, "Backfit Rule Applicability," describes the applicability of the backfit analysis to fuel cycle licensees. The actual backfit analysis would be developed subsequent to the RB as part of the proposed rule package. No change has been made to the RB in response to the comment.

ISSUE 24. RISK ASSESSMENT

NRC-Designated Comment Numbers: 10.5

Comment Summary:
One commenter suggested that licensees should undertake a risk assessment to evaluate the performance of digital systems for confidentiality, integrity, and availability. This would be consistent with NIST SP 800-39, "Managing Information Security Risk" and NIST SP 800-30, "Guide for Conducting Risk Assessments." The commenter suggested that this would provide a more accurate categorization of the systems in question.

NRC's Response:
The NRC staff agrees in part that the proposed rulemaking should require licensees to assess cyber security risk. The NRC staff approach utilizes risk management concepts from NIST SP 800-37. The current approach involves implementation of the risk-management framework which includes: formation of a cyber security team, training staff on cyber security, identification of digital assets associated with potential consequences of concern, application of cyber security controls for digital assets, configuration management of digital assets, cyber security incident response capability, and cyber security event reporting. This approach allows for the application of cyber security controls at either the component or system level, allowing for maximum flexibility to licensees.

Response Summary:
Section 4.4 of the RB has been revised to provide additional detail on the risk management framework and relation to NIST SP 800-37. The back end of the NIST SP 800-37 process (i.e., assessment, authorization, and monitoring) would be further described during the proposed rulemaking process.

ISSUE 25. USE OF NIST STANDARDS

NRC-Designated Comment Number: 10.7 and 10.9

Comment Summary:
One commenter indicated that the use of NIST guidance documents (e.g., NIST SP 800-53) implies that the NRC is going to assume the risk for certain licensee systems. The commenter questions if the NIST standards, which are designed for government agencies, would even be applicable to private industry.

NRC's Response:
The NRC staff disagrees with this comment. The NRC intends to use NIST standards and guidance documents to inform the development of the proposed rule. The NRC staff's use of these standards and guidance documents does not mean that the NRC assumes the risk for the licensees' cyber security programs. Licensees are required to demonstrate adequate protection of health and safety, security and the environment; this includes the area of cyber security. The staff from NRC and NIST have extensively discussed the adaptability of the NIST cyber security standards. During an NRC public meeting on October 22, 2015 (ADAMS Accession No. ML15308A506), NIST staff stated that their standards are adaptable to the private sector. The NRC staff plans to develop regulatory guidance that describes one acceptable approach for licensees to use the NIST standards to support their cyber security programs.

Response Summary:
Section 4.3 of the RB indicates that the proposed rulemaking would consider using nationally recognized and consensus standards such as NIST standards. Information on using these standards would be provided in the guidance for the proposed rule.

ISSUE 26. THE NRC SHOULD STOP WORK ON A NUMBER OF REGULATORY ACTIVITIES

NRC-Designated Comment Numbers: 3.20, 11.10, 11.11, 11.12, 11.13, and 11.14

Comment Summary:
One commenter indicated that the NRC should terminate work on a number of regulatory initiatives that are under development in parallel with the cyber security proposed rulemaking. These included the following items:

- 10 CFR Part 21, Reporting of Defects and Noncompliance;
- effort to develop quantitative dermal and ocular exposure standards;
- 10 CFR Part 73 rulemaking for enhanced security for SNM;
- 10 CFR Part 73 rulemaking for amending material control and accounting regulations; and
- effort to create an ISA Standard.

NRC's Position:
The NRC staff is working on a number of regulatory initiatives including those identified in the comments. These projects are outside the scope of the cyber security proposed rulemaking.

Response Summary:
The comments did not result in any change to the RB.

ISSUE 27. VULNERABILITY MOTIVATING RULEMAKING

NRC-Designated Comment Numbers: 1.4 and 4.5

Comment Summary:
Several commenters asked the NRC to clearly state the vulnerability or threat that is motivating the proposed rulemaking. The commenters indicated they were not aware of any generic or site-specific vulnerabilities that could result in significant impact to safety or security of the public. They also indicated that major cyber security threats should have already been addressed as part of the critical target area (CTA) assessment.

NRC's Position:
Fuel cycle licensees are increasingly using digital assets throughout their operations and in systems important to safety, security, and safeguards. The capabilities exist for malicious actors to exploit network capabilities, wireless interfaces, extensive use of portable media, and the general absence of comprehensive cyber security programs at fuel cycle facilities. NRC regulations do not address cyber security at fuel cycle facilities, other than generic order language which requires certain licensees to address cyber security vulnerabilities but does not specify protection requirements (i.e., cyber security controls). NRC recognizes that industry has implemented voluntary cyber security initiatives. Site visits indicate these programs vary widely between facilities and in some cases are not comprehensive, e.g., employ digital assets that are internet facing, lack basic programmatic controls, lack systematic analysis of potential consequences of concern. The combination of a regulatory gap in the area of cyber security, the licensee's significant dependence upon digital systems, the vulnerability to a cyber security attack, the potential absence of consistent and comprehensive cyber security programs, and the growing capability of malicious actors, has led the NRC staff to propose this high priority, expedited rulemaking.

The NRC staff believes that the proposed cyber security rule should apply to those digital systems and assets that, if compromised, could result in consequences of concern both onsite and offsite. The NRC staff also observes that a CTA assessment does not require comprehensive analysis of digital assets to identify potential consequences of concern.

Response Summary:
The NRC is developing the RB for a proposed cyber security rulemaking to require licensees to implement a robust cyber security program to meet the existing cyber threat. This program involves analyzing digital assets to identify those assets associated with 3S functions. Once identified, digital assets performing 3S functions that, if compromised, could result in a consequence of concern must be protected from a cyber attack.

Appendix A: Table of Comments

This list defines the "NRC-Designated Comment Numbers" (NRC #) for comments received on the draft Regulatory Basis entitled, "Rulemaking for Cyber Security at Fuel Cycle Facilities." The draft Regulatory Basis was published for comment on
September 4, 2015, in the Federal Register (80 FR 53478). NRC staff compiled the table of comments below from the following sources:

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); and
Westinghouse Electric Company LLC letter dated October 5, 2015 (ADAMS Accession No. ML15287A415).

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
1.1	NEI letter dated 10/5/2015 (ML15355A449)	Cyber security is a matter of great national importance. Industry and NRC share a common objective of ensuring that fuel cycle facilities are protected from events that may seriously impact workers, the public, and the environment. As such, we firmly believe that NRC should treat a potential cyber attack like it would treat any other potential initiating event that could also trigger an accident sequence. Licensees have significant expertise in evaluating and mitigating the consequences of accidents through processes, procedures, systems, structures, and components. Significant work and analysis is needed to continue with this effort as the draft Regulatory Basis does not provide a sufficient technical basis to justify rulemaking. In addition to protecting their digital assets for business purposes, licensees are subject to existing security orders requiring that they evaluate and address cyber security vulnerabilities. Further, Category I licensees must protect digital assets for the Design Basis Threat (DBT), which specifically includes a cyber attack. Industry has spent, and continues to spend, significant resources on implementing cyber security programs. These programs continue to evolve in response to changing environments and have sufficiently mitigated the consequences of cyber security breaches without added rulemaking. We trust that this fact is self-evident to NRC as it conducts the site visits currently underway. Rather than dismiss these programs as ad hoc, NRC should evaluate the extent to which existing requirements, in conjunction with ongoing voluntary practices, address the regulatory problem set forth in the draft Regulatory Basis.
1.2	NEI letter dated 10/5/2015 (ML15355A449)	First, the draft Regulatory Basis appears to depart from NRC's historical approach of reflecting the different risks associated with different categories of fuel cycle facilities through different regulatory requirements. The rationale underlying the NRC's security regulations is that protective measures should be commensurate with the potential consequences of malevolent acts to safety and security. The basis for issuing requirements to defend against cyber attacks at fuel cycle facilities that are not currently subject to the DBT requirements in 10 CFR 73.1 must be carefully considered to avoid the unintended adverse effects on diverting limited resources to a single stand-alone focus on cyber security. Rather than follow this traditional approach, the draft Regulatory Basis takes a one-size-fits-all approach of applying cyber security regulations to all fuel cycle facilities regardless of their risk profile, and instead NRC would seek to grade the requirements through implementation guidance. The draft Regulatory Basis does not address this policy issue. While a graded implementation is reasonable, prudent, and desirable, as a matter of policy, NRC should establish requirements reflecting the diverse range of fuel cycle facilities at outset through the rulemaking process rather than deferring this issue to guidance.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
1.3	NEI letter dated 10/5/2015 (ML15355A449)	Second, the draft Regulatory Basis proposes creating requirements that have no nexus to the recognized risks for Category II and III facilities. The objective of the physical protection programs for Category II and III materials is to minimize the possibility for unauthorized removal of SNM and to facilitate the location and recovery of missing SNM. Facilities with Category II and III materials (and uranium hexafluoride conversion facilities) are not required to protect against the DBTs of theft or diversion and radiological sabotage. The NRC has adopted the reasonable position that un-irradiated HEU, LEU, and natural UF6 are not considered a sabotage target. This position was most recently reaffirmed in the 2015 Part 73 Regulatory Basis, which states that there is no need for increased physical security protection of these materials. But here, the draft Regulatory Basis and rulemaking would result in licensees protecting digital assets from a cyber attack where those same assets are not required to be protected against physical attacks. This inconsistency in regulatory approach should not be dismissed without further evaluation. Further, it implies that the threat and consequences of a cyber attack are greater than a physical attack. The draft Regulatory Basis provides no evidence justifying this major shift in the regulatory framework. Before proceeding with a rulemaking, we believe NRC must justify this significant change in its approach to security and address this policy issue.
1.4	NEI letter dated 10/5/2015 (ML15355A449)	Third, Category II and Category III licensees are under orders to identify “Critical Target Areas” (CTAs). A CTA is described as an area that if subjected to a malevolent act, could potentially result in a lethal exposure from radiological material or chemicals subject to NRC regulation to members of the public located outside of the Owner Controlled Area. 3 Licensees used guidance provided by the NRC to identify CTAs and to implement specified protection criteria, if necessary. The NRC has reviewed licensee assessments and implementation of protection measures. No Category III fuel cycle facility has identified a CTA. Industry is not aware of any NRC generic or site-specific vulnerability assessments indicating any cyber threat actuating significant impact on actual safety or security of the public that would justify the current cyber security rulemaking effort. The development of CTAs in accordance with the post-9/11 orders could constitute a reasonable surrogate for a site-specific vulnerability assessment. In the absence of a cyber-specific vulnerability assessment, it seems unreasonable to conclude a cyber attack on a Category III fuel cycle facility could create a CTA that does not otherwise exist. Accordingly, it would appear that requirements to protect against acts of cyber sabotage are simply not justified by the risks.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
1.5	NEI letter dated 10/5/2015 (ML15355A449)	In SRM-SECY-14-0147, the Commission disapproved the staff's recommendation for cyber security orders and directed the staff to initiate a cyber security rulemaking to develop a more fulsome technical basis. Commissioner Ostendorff's vote noted that the "staff has not provided a sufficient basis for the Commission to make a finding that the fuel cycle facilities regulatory functions are not currently protected in a manner sufficient to adequately protect public health and safety." The current draft Regulatory Basis falls far short of providing a detailed rationale to demonstrate that fuel cycle facilities are not adequately protected today. For example, rather than provide significantly new information or a more fulsome assessment of the issues, the draft Regulatory Basis is based on information gathered from site visits in 2011 and discusses cyber event consequences in a vague, non-specific manner. Also, the draft Regulatory Basis continues with an isolated focus on a stand-alone cyber attack. We believe that this approach is not responsive to the SRM direction of ensuring an adequate, integrated look at cyber security as only one aspect of site security. Most importantly, is the draft Regulatory Basis definition of a cyber attack as "having the potential to result in a direct or indirect adverse effect or consequence to a digital asset or system." The purpose of rulemaking and cyber security should be more properly directed to protect against a cyber attack that results in a safety or security consequence of a concern, and not simply a consequence to a digital asset. This broad scope mindset of including all digital assets is not consistent with a risk-informed, graded approach focused on consequences as directed by the SRM. The need to tightly align consequences with the scope of assets protected is at the heart of what has been identified as the most significant lesson learned from implementation of the cyber security requirements for power reactors, and resulted in NEI submitting a petition for rulemaking (PRM-73-18). We have emphasized to NRC on several occasions that such lessons learned must be applied to avoid undue burden to both NRC and industry in this regulatory initiative.
1.6	NEI letter dated 10/5/2015 (ML15355A449)	Specifically address the significant policy issues discussed above, given the lack of analysis that demonstrates the risk for Category II, Category III, and Part 40 fuel cycle facilities. Demonstrate that the shift in the regulatory framework from physical security requirements to cyber security requirements is justified based on increased consequences to the public, worker, or environment.
1.7	NEI letter dated 10/5/2015 (ML15355A449)	Provide clear performance objectives, similar to those found in 10 CFR 70.61, in the Regulatory Basis and rule. Industry provided a comprehensive proposal for a path forward in October 2013. This proposal provided a regulatory basis citing consistency with existing rules, guidance and policy. It contained explicit objectives complimented with clear criteria that enhance the implementation process as well as the inspection of the assessments warranted. The proposal also provided a screening logic that provided a road map for risk informing the assessment to assure the protection of the public, worker and environment. NRC did not provide feedback or a justification on why this proposal was not adequate. We suggest adoption of this approach as opposed to the current path.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
1.8	NEI letter dated 10/5/2015 (ML15355A449)	As discussed above, the rulemaking should be "right sized" from the beginning with the end state in mind. Currently, the draft Regulatory Basis casts a wide net capturing all digital assets and relies on screening contained in guidance to ensure the "right end state" of targeted digital assets will reveal itself. The scope of assets identified in the regulations requiring protection should only extend to those most necessary to prevent theft or sabotage of SNM. NEI recommends that NRC consider the specific recommendations in PRM-73-18 (79 FR 183, dated September 22, 2014) as a basis for the scoping provisions. We believe this recommendation is consistent with SECY-14-0147, which states: "The results of this [PRM] activity will be considered to the extent relevant to FCFs if rulemaking is pursued for FCFs." The Regulatory 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.
1.9	NEI letter dated 10/5/2015 (ML15355A449)	Rather than issuing specific cyber reporting requirements, the NRC should carefully assess existing reporting requirements applicable to fuel cycle facilities to determine if they are adequate to cover reporting of cyber security events since such requirements focus on the safety/security results of a failed safety device regardless of the initiating event. Existing guidance on applicable reporting requirements could be revised to address cyber events.
1.10	NEI letter dated 10/5/2015 (ML15355A449)	In the Regulatory Basis, NRC should provide a quantitative assessment on the consequences of a cyber security event. In its absence, industry is considering whether it should convene an expert panel to quantify the risks from a cyber attack. Based on our consideration of this issue to date, preliminary indicators could lead to a conceivable finding that a minimal, if any, increased safety margin is gained following implementation of the approach described in the draft Regulatory Basis.
1.11	NEI letter dated 10/5/2015 (ML15355A449)	Any new regulation should not apply to all digital assets managed by a licensee under the purview of another agency's oversight (e.g. DOE, NNSA, DOD) that are accredited under an established national consensus standard or that other agency's cyber program. Otherwise these program areas will be subject to unnecessary dual regulation. Therefore, the final rule and regulatory basis should include a specific exemption for these licensee programs.
1.12	NEI letter dated 10/5/2015 (ML15355A449)	Part 73 requires that certain licensees protect SNM. However, these requirements do not apply to Part 40 licensees. Accordingly, uranium hexafluoride conversion facilities should be explicitly excluded from this rulemaking. The lack of an identified CTA is indicative of the low risk to the safety and security of these facilities from a cyber attack clearly supports this exclusion.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
1.13	NEI letter dated 10/5/2015 (ML15355A449)	The draft Regulatory Basis provides no substantive discussion of the backfitting considerations, and dispenses with any meaningful costs justification to an unsubstantiated conclusion that, “a rulemaking to implement cyber security requirements for FCF licensees will have a number of benefits that justify the potential cost impacts both on the licensee and the NRC.” This improper justification implies that whatever the cost to licensees, the safety and compliance benefits of the rulemaking are worth it. At best, this rulemaking would marginally improve safety but at great financial cost and at the expense of other licensee self-identified operational improvements, which on a site-specific basis often have a higher rate of return to safety. At a closed Commission briefing in February 2014, two power reactor licensees provided a detailed description of their current expenditures required to comply with the power reactor cyber security requirements. Both licensees indicated that the current and projected full program implementation costs substantially exceed the cost estimates provided in the regulatory analysis for the rulemaking included in Enclosure 2 to SECY-08-0099 (July 9, 2008). The regulatory analysis for reactors estimated a one-time cost for program establishment of $1,194,200 per site. A key driver for the costliness of compliance is the large number of digital assets identified for protection against cyber attack that have no nexus to preventing radiological sabotage. Given the draft Regulatory Basis could require fuel cycle facilities to protect an even broader set of assets than the power reactors, it is reasonable to conclude that the costs to fuel cycle facility licensees will be considerable. The cost implications for Category II and Category III licensees may be even greater given these facilities do not have NRC-required access authorization, physical protection, and insider mitigation programs that the reactor and Category I licensees may credit for affording a certain degree of cyber security protection. Unless cyber security requirements are justified by a substantial increase in overall protection of public health, safety, or security, and the implementation costs for facilities are justified in view of this increased protection, NRC should not proceed with this rulemaking.
2.1	NEI Attachment 1 dated 10/5/2015 (ML15355A450)	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).”
2.2	NEI Attachment 1 dated 10/5/2015 (ML15355A450)	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.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
2.3	NEI Attachment 1 dated 10/5/2015 (ML15355A450)	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.
2.4	NEI Attachment 1 dated 10/5/2015 (ML15355A450)	It is unnecessary to include emergency preparedness (EP) functions with 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 requirements.
2.5	NEI Attachment 1 dated 10/5/2015 (ML15355A450)	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.
2.6	NEI Attachment 1 dated 10/5/2015 (ML15355A450)	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.
2.7	NEI Attachment 1 dated 10/5/2015 (ML15355A450)	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).

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
2.8	NEI Attachment 1 dated 10/5/2015 (ML15355A450)	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.
2.9	NEI Attachment 1 dated 10/5/2015 (ML15355A450)	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.
2.10	NEI Attachment 1 dated 10/5/2015 (ML15355A450)	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.”).

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
2.11	NEI Attachment 1 dated 10/5/2015 (ML15355A450)	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.
2.12	NEI Attachment 1 dated 10/5/2015 (ML15355A450)	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."

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
2.13	NEI Attachment 1 dated 10/5/2015 (ML15355A450)	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).
2.14	NEI Attachment 1 dated 10/5/2015 (ML15355A450)	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.
2.15	NEI Attachment 1 dated 10/5/2015 (ML15355A450)	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.
2.16	NEI Attachment 1 dated 10/5/2015 (ML15355A450)	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.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
2.17	NEI Attachment 1 dated 10/5/2015 (ML15355A450)	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 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."
2.18	NEI Attachment 1 dated 10/5/2015 (ML15355A450)' ,	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.
3.1	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	Response to NRC Objective 1: This objective is unnecessary because Category I fuel cycle facilities are already subject to the DBT, which includes a cyber attack as an adversary attribute. This rulemaking would, however, determine the extent to which explicit programmatic requirements are necessary. The NRC staff has not adequately justified the proposed broad scope of SSEPMCA functions that must be protected from a cyber attack. The stated purpose of the rulemaking effort is to establish new cyber security regulations for fuel cycle facilities in Part 73. Part 73 prescribes requirements for the establishment and maintenance of a physical protection system which will have capabilities for the protection of special nuclear material. The general performance objectives for the protection of SSNM 10 CFR 73.20 states: "The physical protection system shall be designed to protect against the design basis threats of theft or diversion of strategic special nuclear material and radiological sabotage as stated in § 73.1(a)." The draft regulatory basis provides little discussion of why protecting digital assets associated with each element of SSEPMCA functions against the DBT cyber attack are necessary to ensure the capability to protect against theft, diversion, or sabotage. Notably, the draft regulatory basis provides no compelling evidence that a cyber attack on Category I fuel cycle facilities would likely result in theft, diversion, or sabotage.
3.2	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	Rather than protecting digital assets associated with SSEPMCA functions, the cyber security requirements should extend only to those digital assets whose compromise by cyber attack would likely result in theft, diversion, or sabotage. This comment reflects what the industry has identified as the most significant lesson learned from the implementation of cyber security requirements at power reactors, and that resulted in the industry submitting a petition for rulemaking (PRM-73-18). SECY-14-0147 states that this rulemaking effort would consider the results of that petition to the extent relevant. Protecting those assets necessary to prevent theft, diversion, or sabotage ensures the public health and safety can be maintained without requiring licensees to protect an overly broad set of equipment, and allows licensees the ability to focus resources on the protection of digital assets that have a nexus to radiological safety and security.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
3.3	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	The rulemaking should prevent overlap with Department of Energy (DOE) security requirements. Certain fuel cycle facilities (Category I and Category III enrichers) are required to implement DOE cyber security requirements. The draft regulatory basis states, "The NRC staff currently anticipates that digital assets that reside in DOE accredited networks or systems authorized to handle classified information will be excluded from the requirements of the proposed rule." This exemption should be codified in the final requirements and enhanced to include non-classified accredited systems as well.
3.4	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	Response to NRC Objective 2: This objective involves a substantial deviation from and conflicts with the current material categorization approach, and does not appear fully informed by the post-9/11 order activities. The draft regulatory basis does not justify this objective. The objective of the physical protection system for Category II and III materials is to minimize the possibility for unauthorized removal of SNM and to facilitate location and recovery of missing SNM. The NRC's policy is not to require the physical protection systems of facilities with Category II and III materials and non-power reactors to protect against the DBTs of theft or diversion and radiological sabotage, and indeed, the NRC maintains that un-irradiated HEU, LEU, and natural UF6 are not a sabotage target. Rather, for these facilities, the NRC's policy is to require licensees to meet a set of requirements, the effectiveness of which have been evaluated based on NRC threat assessments as well as consequence and security assessments for these facilities. The NRC's recently completed regulatory basis for enhanced security of SNM (NRC Docket ID: NRC-2014-0118) has reaffirmed this position. Accordingly, this objective is inappropriate.
3.5	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	Should the NRC conclude that cyber security program requirements are necessary for non-Category I licensees, the requirements should extend only to those digital assets necessary to meet the performance objectives in 10 CFR 73.67 for the protection of SNM – and not the overly broad scope of any digital asset associated with SSEPMCA functions.
3.6	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	The cost considerations in the draft regulatory basis provide no cost estimates or justification that the expected implementation cost is justified by the risks.
3.7	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	The draft regulatory basis does not describe how the NRC would differentiate the high-assurance requirement proposed for Category I facilities from the reasonable assurance requirements proposed for the other facilities. See 44 Fed. Reg. 68,185 (Nov. 28, 1979), noting that the "high assurance" standard "is deemed to be comparable to the degree of assurance contemplated by the Commission in its safety review for protection against severe postulated accidents having potential consequences similar to the potential consequences from reactor sabotage" and that the "reasonable assurance" standard itself "varies with the gravity of the safety concern"). A high assurance standard is not appropriate for Category I licensees.
3.8	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	The NRC has no security requirements under Part 73 for facilities licensed under Part 40, which do not possess SNM. Further, Part 40 licensees were required by the orders to identify CTAs – and there is currently no identified CTA at a Part 40 licensed facility. Accordingly, this rulemaking should explicitly exclude Part 40 licensees.
3.9	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	The response in the bullet above regarding Category I facilities discusses industry's additional concerns with the use of SSEPMCA as a scoping criteria. These same concerns apply to Category II, Category III, and Part 40 licensees.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
3.10	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	Response to NRC Objective 3: A simple codification of the post-9/11 orders may not be warranted. The draft regulatory basis indicates the orders focused on computer systems that conduct and maintain communications during emergency response actions. The regulatory basis provides little discussion of how the proliferation and diversity of modern communications technologies (e.g., cellular phones) may obviate the need for explicit requirements that may have been appropriate at the time. As discussed earlier in these comments, the post-9/11 orders required the identification of CTAs. The draft regulatory basis provides no discussion of how CTA concepts are being addressed, particularly the consequences considered for CTAs of lethal exposure from radiological material or chemicals to members of the public located outside of the Owner Controlled Area (OCA). In January 2015, the NRC finalized a regulatory basis for enhanced security of SNM. This effort included codification of the post-9/11 orders. This effort did not result in increased physical security requirements for Category II or Category III SNM at fixed sites. The draft regulatory basis for cyber security does not provide a justification that explicit cyber requirements are necessary to codify the post-9/11 orders where there was no corresponding recommendation to increase physical security requirements.
3.11	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	Response to NRC Objective 4: The imposition of new requirements must be justified by the costs and applicable backfitting considerations. Before proceeding to codify orders or the industry voluntary actions, the NRC should ensure the safety benefit is justified in light of a value-impact estimate and backfitting considerations. Should the conclusion be reached that requirements are necessary for each category of affected licensee, the regulatory analysis should consider whether voluntary actions provide a similar level of protection.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
3.12	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	Response to NRC Objective 5: A graded, performance-based framework is prudent, but the framework should also be risk-informed, and rely on the current material categorization approach the NRC currently uses to grade security measures for the protection of SNM. The draft regulatory basis provides little discussion of how the proposed requirements would be graded by facility type, and there is a strong indication that this grading will be performed through guidance, rather than through the regulation. Different security requirements under Part 73 are already established for each facility type, and the grading of cyber security requirements should be integrated into these existing security requirements. Specifically, the scope and performance objective for each category of licensee should be explicitly stated within the regulation, and not relegated to guidance. Based on the current material categorization approach and security requirements under Part 73, it would appear that the performance objectives the NRC should be considering in the regulatory basis are as follows: • Category I facilities - prevent theft or diversion and radiological sabotage (10CFR73.20). • Category II and III facilities – ensure the capability to detect the unauthorized removal of large quantities of SNM (10CFR73.67). • Part 40 licensees – no performance objective and no cyber security requirements. The consequences of concern should be tied directly to these performance criteria, and a justification provided in the regulatory basis. Deviations from the consequence criteria provided in the post-9/11 orders must be strongly justified. Explicit exemptions should exist within the regulation to avoid duplication of requirements with licensees subject to DOE cyber security requirements.
3.13	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	Response to NRC Objective 6: Fuel cycle facilities are already subject to reporting requirements that cover degraded facility conditions and security events. These current requirements should be evaluated by the NRC to determine if they are adequate to address the reporting of cyber attacks. Rather than revising or issuing new requirements, revisions to regulatory guidance could achieve the desired outcome with reduced burden on the NRC and its licensees.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
3.14	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	Response to Question Section III-2: The draft regulatory basis diverges from the current regulatory framework the NRC has used to grade the security requirements using a material categorization approach. This deviation is not justified in the regulatory basis. Our substantive concerns with this deviation is provided in the response above. Furthermore, even if the NRC staff provided a basis for departing from its traditional material categorization approach, it should consider alternatives involving reliance on voluntary industry actions to complement existing requirements. Rulemaking may not be required to achieve NRC's objectives. In addition to protecting their digital assets for business purposes, licensees are subject to existing security orders requiring that they evaluate and address cyber security vulnerabilities. Further, Category I licensees must protect digital assets under for the DBT, which specifically includes a cyber attack. Industry has spent, and continues to spend, significant resources on implementing cyber security programs. These programs continue to evolve in response to changing environments and have sufficiently mitigated the consequences of cyber security breaches. We trust that this fact is self-evident to NRC as it conducts the site visits currently underway. Rather than dismiss these programs as ad hoc, NRC should evaluate the extent to which existing requirements, in conjunction with ongoing voluntary practices, provide a viable alternative to address the regulatory problem set forth in the draft Regulatory Basis.
3.15	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	If the NRC decides a rulemaking is necessary, there are alternative rulemaking approaches it should consider. Based on the current material categorization approach and security requirements under Part 73, NRC should develop an alternate approach for cyber security requirements based on the following performance objectives: • Category I facilities - prevent theft or diversion and radiological sabotage (10CFR73.20). • Category II and III facilities – ensure the capability to detect the unauthorized removal of large quantities of SNM (10CFR 73.67). • Part 40 licensees – no performance objective and no cyber security requirements.
3.16	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	The NRC should also consider an alternative approach to information protection that relies on security systems used by licensees to implement requirements under 10 CFR 95 for information security. The draft regulatory basis provides no indication that the current requirements in Part 95 are inadequate to protect national security information or restricted data, or that the proposed requirements under Part 73 are the solution to the problem under Part 95. Addressing this issue should be pursued under a separate rulemaking. Additionally, industry provided a proposal for a path forward in October 2013 that was based on 70.61 performance objectives, with modifications for EP and MC&A, which set objectives as a high consequence event. NRC did not provide feedback or a justification on why this proposal was not adequate.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
3.17	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	Response to Question Section III-3: The draft regulatory basis lacks sufficient detail that would allow for estimating the expected costs. As a point of reference in developing the cost estimates for the draft regulatory analysis, the NRC should consider the detailed cost estimate for cyber-security implementation at power reactors provided in Enclosure 2 to SECY-2008-0099 (ML081650474). By all indications, there would appear to be substantial similarities between the power reactor cyber security requirements and those being proposed in the draft regulatory basis. At a closed Commission briefing in February 2014, two power reactor licensees provided a detailed description of their current expenditures required to comply with the power reactor cyber-security requirements. Both licensees indicated that the current and projected full program implementation costs substantially exceed the cost estimates provided in the regulatory analysis for the rulemaking included in Enclosure 2 to SECY-08-0099. Based on the power reactor experience, the estimates in the SECY could reasonably be increased by a factor of 5 to 10. The cost implications for Category II, Category III, and Part 40 licensees may be even greater given these facilities do not have established access authorization, physical protection, and insider mitigation programs that the reactor and Category I licensees may credit for affording a certain degree of cyber-security protection. Unless cyber security requirements are justified by the risks, these increased compliance costs both reduce the international competiveness of fuel cycle facilities, and negatively impact the price-competitiveness of nuclear power plants in an already challenging energy market. Chapter 8 provides no indication of the net safety or security benefit to be gained by the implementation of the proposed rule. NEI recommends the NRC consider the guidance in NUREG/BR-0058, “Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission” in developing a more fulsome analysis of the expected values and impacts.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
3.18	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	Response to Question Section III-4: As indicated in the draft regulatory basis, fuel cycle facilities have implemented cyber security programs. These programs have, in large part, been established to address business risk. The draft regulatory basis describes two cyber attacks on industrial facilities as indicative of the need for cyber security requirements at fuel cycle facilities – yet the draft regulatory basis provides no indication of the potential safety or security concerns associated with these attacks. It should be noted that neither attack had a reported consequence to the public or worker. In the case of attack on Natanz, the impact was the destruction of roughly 1,000 centrifuges, but no reported radiological or chemical exposure. This attack provides a clear example of the business drivers for cyber security to protect business investments. Regarding the attack on, Saudi Aramco that disabled 30,000 workstations - CEO Khalid al-Falih said in a statement: "We would like to emphasize and assure our stakeholders, customers and partners that our core businesses of oil and gas exploration, production and distribution from the wellhead to the distribution network were unaffected and are functioning as reliably as ever." There is a clear business need to address cyber security, and the industry, as evidenced in the NRC's site visits, have expended considerable resources to address those business risks. The draft regulatory basis provides no compelling evidence that a cyber attack on a fuel cycle facility would be inimical to the common defense and security. Industry is unconvinced that the markets and business drivers do not provide sufficient motivation for investment in cyber security. Nor has NRC given serious consideration to whether voluntary industry actions would provide a reasonable means to address the concerns in the draft regulatory basis. And if the NRC concludes that voluntary industry efforts are inadequately protective, the NRC should establish a clear performance objective, and should analyze any gap. NEI recommends the NRC consider using NUREG/BR-0058, "Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission" as a tool in performing this assessment.
3.19	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	Response to Question Section IV-1: Given the short comment period and the draft regulatory basis' lack of detail that would allow for estimating the expected implementation timeline required it is not possible to provide an informed recommendation. Therefore, we suggest an implementation schedule that recognizes the unique programs and challenges that fuel cycle facilities may face during implementation. Similar to the implementation of 10 CFR 73.54 for reactors, we propose that licensees be given 6 months from the date of publication of the rule to submit a cyber security plan that satisfies the requirements of the regulations for Commission review and approval and a proposed implementation schedule.
3.20	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	Response to Question Section IV-2: To address CER challenges, NRC should move quickly to implement the Commission's direction on Project AIM and use industry's feedback [September 15, 2015, John Butler (NEI) to Frederick Brown (NRC); Industry Recommendations for NRC Project AIM 2020 Prioritization and Re-baselining Initiatives] on NRC's Common Prioritization and Re-baselining initiatives. Industry identified several rulemakings and other regulatory initiatives related to fuel cycle facilities that are of low safety significance.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
3.21	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	Response to Question Section IV-3: The oversight of certain digital assets are currently accredited under an established national consensus standard under the purview of another agency's oversight (i.e. DOE, NNSA, DOD). This regulation should not apply to digital assets managed by a licensee under another agency's cyber program. Otherwise these program areas will be subject to dual regulation which cannot be justified in the absence of a significant increase in safety or security. Therefore, the final rule and regulation basis should include a specific exemption for these licensee programs.
3.22	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	Response to Question Section IV-4: Without a clear technical basis that fully describes the consequences and performance objectives, the industry is not well served by the diversion of limited resources to meet current and/or other proposed regulatory requirements that are of low or negligible safety significance at the expense of making self-identified operational improvements, which on a site-specific basis often result in greater safety and security benefits.
3.23	NEI Attachment 2 dated 10/5/2015 (ML15355A452)	Response to Question Section IV-5: The draft regulatory basis lacks significant detail that would allow for estimating the expected costs. At best, this rulemaking would incrementally improve safety at great resource cost at the expense of operation improvements that licensees have self-identified, which many times on a site specific basis have a higher rate of return to safety. As a point of reference in developing the cost estimates for the final regulatory analysis, the NRC could consider the detailed cost estimate for cyber security implementation at power reactors provided in Enclosure 2 to SECY-2008-0099 (ML081650474). By all indications, there would appear to be substantial similarities between the power reactor cyber security requirements and those being proposed in the draft regulatory basis. Based on the power reactor experience, the estimates in the SECY could reasonably be increased by a factor of 5 to 10. The cost implications for Category II, Category III, and Part 40 licensees may be even greater given these facilities do not have established access authorization, physical protection, and insider mitigation programs that the reactor and Category I licensees may credit for affording a certain degree of cyber security protection.
4.1	AREVA NP, Inc. letter dated 10/5/2015 (ML15287A413)	The current draft Regulatory Basis does not provide a sufficient technical basis to support rulemaking without further detailing the technical justification of the safety program impacts and their relative value in maintaining adequate safety/security margin.
4.2	AREVA NP, Inc. letter dated 10/5/2015 (ML15287A413)	The matter of cyber security is of great international importance. AREVA understands its obligation to the objective of ensuring its fuel cycle facility protects the public, worker, and environment from consequences of concern consistent with historic regulatory standards. AREVA considers a cyber attack simply as another category of initiating event in an accident sequence. Only licensees have significant expertise in evaluating and mitigating the consequences of accidents through processes, procedures, systems, structures, and components for their facilities. The current draft Regulatory Basis does not provide a sufficient technical basis to support rulemaking without further detailing the technical justification of the safety program impacts and their relative value in maintaining adequate safety/security margin. AREVA, in addition to protecting its digital assets for business purposes, is compliant with existing security Orders directing it to evaluate and address cyber security vulnerabilities. AREVA has spent, and continues to spend, significant resources on implementing cyber security programs that continue to evolve and have sufficiently mitigated the consequences of cyber security breaches.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
4.3	AREVA NP, Inc. letter dated 10/5/2015 (ML15287A413)	AREVA supports the NEI's (ref. NEI letter from Joseph E. Pollock dated October 5, 2015) representation that the cyber threat for fuel cycle facilities should be informed by and consistent with NRC's historical approach and overall framework for the protection of special nuclear material. The draft Regulatory Basis does not address this apparent policy issue, but instead takes the approach of applying cyber security requirements to all fuel cycle facilities regardless of their risk profile, and would seek to grade the implementation through guidance. While a graded and risk-informed implementation is reasonable, prudent and desirable, the applicability of diverse requirements to the range of fuel cycle facilities is a matter of policy best addressed through the rulemaking process and not relegated to guidance.
4.4	AREVA NP, Inc. letter dated 10/5/2015 (ML15287A413)	The objective of the physical protection system for Category III materials is to minimize the possibility for unauthorized removal of SNM and to facilitate the location and recovery of missing SNM. Facilities with Category III materials are not required to protect against the Design Basis Threats (DBTs) of theft or diversion and radiological sabotage. The NRC has historically held that un-irradiated LEU, nor natural UF6, is considered a sabotage target. This was most recently reaffirmed in the 2015 Part 73 Regulatory Basis, which states that there is no need for increased physical security protection for these materials. The draft Regulatory Basis and rulemaking would result in licensees protecting digital assets from a cyber attack where those same assets are not required to be protected against physical attacks. This apparent inconsistency in regulatory approach should not be dismissed without further evaluation. Further, it implies that the threat and consequences of a cyber attack are greater than a physical attack. The draft Regulatory Basis provides no quantitative nor convincing qualitative evidence that this quantum leap in the regulatory framework is justified by the risk. AREVA believes this is a policy issue that must be addressed in the rulemaking.
4.5	AREVA NP, Inc. letter dated 10/5/2015 (ML15287A413)	The AREVA Richland Fuel Manufacturing site is under orders to identify "Critical Target Areas" (CTAs). AREVA used guidance provided by the NRC to identify CTA's and to implement specified protection criteria if necessary. In the NEI letter from Joseph E. Pollock dated October 5, 2015. NEI stated that no Category III fuel cycle facility has identified a CTA. AREVA is not aware of any NRC generic or site-specific vulnerability assessments indicating any cyber threat actuating significant impact on actual safety or security of the public that would justify the current cyber security rulemaking effort. The development of CTAs in accordance with the post- 9/11 orders could constitute a reasonable surrogate for a site-specific vulnerability assessment. In the absence of a cyber-specific vulnerability assessment, it seems unreasonable to conclude a cyber attack on a Category III fuel cycle facility could create a CTA that does not otherwise exist. Accordingly, it would appear that requirements to protect against acts of cyber sabotage are simply not justified by the risks

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
4.6	AREVA NP, Inc. letter dated 10/5/2015 (ML15287A413)	AREVA supports the Commission's direction to the staff to proceed with rulemaking with the expectation that the rulemaking process would allow for a full vetting of the concerns held by the fuel cycle industry in this matter. But the fact is that the current draft Regulatory Basis provides no significantly new information or detailed rationale to demonstrate that fuel cycle facilities are not adequately protected today. The draft Regulatory Basis discusses cyber event consequences in a vague, non-specific manner. Also, the draft Regulatory Basis continues with a singular focus on the cyber attack vs. the consequences that both AREVA and the agency are bound to prevent to the public, worker and environment. AREVA believes that this approach is not responsive to the SRM direction of ensuring an adequate, integrated look at cyber security as only one aspect of site security. The purpose of rulemaking and cyber security should be to protect against a cyber attack that results in a safety or security consequence of concern to the public, worker or environment, and not simply a consequence to a digital asset. Yet the Regulatory Basis document definition of a cyber attack as "having the potential to result in a direct or indirect adverse effect or consequence to a digital asset or system" demonstrates the inappropriate focus on the wrong thing. This mindset focusing on the digital asset vs. the consequences of an event to the public, worker or environment is not consistent with a risk-informed graded approach as directed by the SRM.
4.7	AREVA NP, Inc. letter dated 10/5/2015 (ML15287A413)	AREVA supports the principle of using lessons learned and the case of the recent reactor cyber rule reveals some important pitfalls to prevent. The need to tightly align consequences with the scope of assets protected is at the heart of what has been identified as the most significant lesson learned from implementation of the cyber security requirements for power reactors, and one that resulted in NEI submitting a petition for rulemaking (PRM-73-18) to address.
4.8	AREVA NP, Inc. letter dated 10/5/2015 (ML15287A413)	AREVA disagrees with the oversimplified cost justification statement that "a rulemaking to implement cyber security requirements for FCF licensees will have a number of benefits that justify the potential cost impacts both on the licensee and the NRC." AREVA believes it is critically flawed by implying that whatever the cyber rulemaking licensee cost, the safety and compliance benefits are worth it. This logic would incrementally improve safety at a great resource cost at the expense of operational improvements that AREVA has self-identified and is confident have a higher rate of return to safety. While the Regulatory Analysis has yet to be performed, a key driver for the costliness of compliance is the large number of digital assets identified by the Regulatory Basis document for protection against cyber attack that have no nexus to preventing radiological sabotage. The cost implications for Category III licensees may be even greater than reactors or Category I FCF's given Cat III facilities do not have the same requirements for access authorization, physical protection, and insider mitigation programs that the reactor and Category I licensees may credit for affording a certain degree of cyber security protection. Unless cyber security requirements are justified by the risks, these increased compliance costs misdirect limited resources and reduce the international competiveness of fuel cycle facilities, and negatively impact the price-competitiveness of nuclear power plants in an already challenging energy market.
4.9	AREVA NP, Inc. letter dated 10/5/2015 (ML15287A413)	AREVA Recommendation 1: Specifically address the significant policy issues discussed above, given the lack of analysis that demonstrates the risk for Category II, Category III, and Part 40 fuel cycle facilities. Demonstrate that the shift in the regulatory framework from physical security requirements to cyber security requirements is justified based on increased consequences to the public, worker, or environment.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
4.10	AREVA NP, Inc. letter dated 10/5/2015 (ML15287A413)	AREVA Recommendation 2: Provide clear performance objectives, similar to those found in 10 CFR 70.61, in the Regulatory Basis and rule. Industry provided a comprehensive proposal for a path forward in October 2013. This proposal provided a regulatory basis citing consistency with existing rules, guidance and policy. It contained explicit objectives complemented with clear criteria that enhance the implementation process as well as subsequent assessments. The proposal also provided a screening logic that provided a road map for risk informing the assessment to assure the protection of the public, worker and environment. NRC did not provide feedback or a justification on why this proposal was not adequate. We suggest adoption of this approach as opposed to the current path.
4.11	AREVA NP, Inc. letter dated 10/5/2015 (ML15287A413)	AREVA Recommendation 3: As discussed above, the rulemaking should be "right sized" from the beginning with the end state in mind. Currently, the draft Regulatory Basis casts a wide net capturing all digital assets and relies on screening contained in guidance to ensure the "right end state" of targeted digital assets will reveal itself. The scope of assets identified in the regulations requiring protection should only extend to those most necessary to prevent theft or sabotage of SNM. NEI recommends that NRC consider the specific recommendations in PRM-73-18 (79 FR 183, dated September 22, 2014) as a basis for the scoping provisions. We believe this recommendation is consistent with SECY-14-0147, which states: "The results of this [PRM] activity will be considered to the extent relevant to FCFs if rulemaking is pursued for FCFs." The Regulatory 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.
4.12	AREVA NP, Inc. letter dated 10/5/2015 (ML15287A413)	AREVA Recommendation 4: Rather than issuing specific cyber reporting requirements, the NRC should carefully assess existing reporting requirements applicable to fuel cycle facilities to determine if they are adequate to cover reporting of cyber security events since such requirements focus on the safety/security results of a failed safety device regardless of the initiating event. Existing guidance on applicable reporting requirements could be revised to address cyber events.
4.13	AREVA NP, Inc. letter dated 10/5/2015 (ML15287A413)	AREVA Recommendation 5: In the Regulatory Basis, NRC should provide a quantitative assessment of the consequences of a cyber security event. In its absence, industry is considering whether it should convene an expert panel to quantify the risks from a cyber attack. Based on our consideration of this issue to date, preliminary indicators could lead to a conceivable finding that a minimal, if any, increased safety margin is gained following implementation of the approach described in the draft Regulatory Basis.
4.14	AREVA NP, Inc. letter dated 10/5/2015 (ML15287A413)	AREVA Recommendation 6: Any new regulation should not apply to all digital assets managed by a licensee under the purview of another agency's oversight (e.g. DOE, NNSA, DOD) that are accredited under an established national consensus standard or that other agency's cyber program. Otherwise these program areas will be subject to unnecessary dual regulation. Therefore, the final rule and regulatory basis should include a specific exemption for these licensee programs.
4.15	AREVA NP, Inc. letter dated 10/5/2015 (ML15287A413)	AREVA Recommendation 7 Part 73 requires that certain licensees protect SNM. However, these requirements do not apply to Part 40 licensees. Accordingly, uranium hexafluoride conversion facilities should be explicitly excluded from this rulemaking. The lack of an identified CTA is indicative of the low risk to the safety and security of these facilities from a cyber attack and clearly supports this exclusion.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
4.16	AREVA NP, Inc. letter dated 10/5/2015 (ML15287A413)	AREVA also supports the detailed comments and FRN question/answers as submitted by NEI in the letter from Joseph E. Pollock dated October 5, 2015.
4.17	AREVA NP, Inc. letter dated 10/5/2015 (ML15287A413)	AREVA strongly suggests a reconsideration of the industry proposal submitted in October 2013 for further development to accomplish the common goal of safety and security in this matter.
5.1	BWXT letter dated 10/5/2015 (ML15292A560)	BWX Technologies, Inc., Nuclear Operations Group- Lynchburg (BWXT NOG-L) fully endorses the letter submitted by the Nuclear Energy Institute (NEI) on October 5, 2015 (Reference 1) regarding the Nuclear Regulatory Commission's (NRC) Fuel Cycle Facility Cyber Security Draft Regulatory Basis (80 FR 53478) [Docket 2015-0179] (Reference 2).
5.2	BWXT letter dated 10/5/2015 (ML15292A560)	The Federal Register Notice (FRN) was issued on September 4, 2015 and provided the draft Regulatory Basis for public comment by October 5, 2015. The NEI letter incorporates feedback from BWXT NOG-L in the industry comments attachments. BWXT NOG-L recently hosted a NRC Cyber Security team visit to review the status of cyber security voluntary action implementation. Nuclear Fuel Services (NFS) was also represented in the review and provided the NRC team a description of similarities and differences between the NOG-L and NFS facilities. This visit occurred during the week of September 28, 2015 and we hope the information gained during the visit was beneficial for the NRC team. It is our intent to continue working with the NRC to improve overall Cyber Security and protect critical infrastructure by actively participating in the rulemaking process.
6.1	GNFA letter dated 10/5/2015 (ML15287A416)	The fuel cycle industry has recognized the need for cyber security and voluntary cyber security control actions that have been and continue to be implemented for a variety of reasons including safety, compliance, business continuity, and the protection of company sensitive or classified information. However, as a Category Ill fuel fabrication facility, we are concerned that several of the proposed changes are overly broad, difficult to implement and may have a significant impact on GNF-A operations without a clear performance objective, demonstrated need, or security concern.
6.2	GNFA letter dated 10/5/2015 (ML15287A416)	The NRC draft regulatory basis document for fuel cycle facilities contains no performance objective. 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. The industry, in earlier discussions with the staff and in written comments, suggested consequences of concern to establish 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.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
6.3	GNFA letter dated 10/5/2015 (ML15287A416)	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 (i.e. requiring protection of the digital asset itself rather than prevention or mitigation of a defined consequence). 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 (i.e. preventing radiological sabotage that could cause significant core damage or affecting safe shutdown margin) 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.
6.4	GNFA letter dated 10/5/2015 (ML15287A416)	Determining the consequences of concern is absolutely necessary to risk-inform which digital assets require protection from a cyber attack. We acknowledge that there has been some effort to provide further definition in this area; however, we continue to believe that further details are needed prior to issuance and implementation of new requirements. The NRC staff questionnaire and site visits considered the status of licensees' cyber security systems and practices, but did not consider the analysis of the impact or result of a cyber attack on each licensee's operational safety or security. One critical step in the assessment of the regulatory need is to assess the risk to safe and secure operations as a result of credible cyber threats. The industry supports this element as a prerequisite to regulatory action in order to inform the scope and degree of necessary actions to assure safety. We encourage the staff to allow each licensee to perform vulnerability and consequence analyses that could directly risk inform a digital asset screening process.
6.5	GNFA letter dated 10/5/2015 (ML15287A416)	The scope of the implementation should be limited to operational equipment rather than information assets. The draft regulatory basis includes the protection of "information processing systems" (e.g., MC&A databases), "support system and/or digital assets associated with SSEPMCA functions" and "communication systems". This imposes on fuel cycle facilities a level of protection exceeding existing security requirements and those addressing the threat of cyber attack. For example, it needs to be better stated why a cyber attack on material control and accounting (MC&A) functions would be subject to additional cyber protection, as each licensee must have a physical protection plan that is independent of the MC&A plan to assure diversion of SNM is highly unlikely. In addition, a compromise affecting the functionality of a "support system" or "communication system" does not create a consequence of concern where safe shutdown or compensatory actions can be immediately taken.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
6.6	GNFA letter dated 10/5/2015 (ML15287A416)	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.” 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. Other cyber security guidance documents may be more appropriate for FCF facilities than NIST 800-53 (i.e. 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)”
6.7	GNFA letter dated 10/5/2015 (ML15287A416)	Section 3.3, page 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.” Contrary to the above statement in the draft regulatory basis, the fuel cycle industry used a variety of formal standards including ISA/IEC standards, ISO based corporate policies, DOE orders or CNSS instructions to implement the voluntary cyber security initiatives.
6.8	GNFA letter dated 10/5/2015 (ML15287A416)	Section 4.3, page 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” Because 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 licensee impact. 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).

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
6.9	GNFA letter dated 10/5/2015 (ML15287A416)	Section 8.6, page 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 benefits with protecting the functionality of certain SSEPMCA digital assets. Second, there is no justification 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”.
7.1	Honeywell letter dated 10/2/2015 (ML15287A414)	Honeywell endorses and incorporates the comments on the proposed rulemaking submitted by NEI.
7.2	Honeywell letter dated 10/2/2015 (ML15287A414)	Honeywell International, Inc. ("Honeywell") is submitting these comments regarding the NRC' s draft regulatory basis in support of a rulemaking that would amend NRC regulations by adopting new cyber security requirements for certain nuclear fuel cycle facilities, including uranium hexafluoride conversion facilities. At the outset, Honeywell endorses and incorporates the comments on the proposed rulemaking submitted by the Nuclear Energy Institute ("NEI"). Honeywell believes that the cyber security rulemaking effort should be discontinued for uranium hexafluoride conversion facilities given the significant policy issues discussed in NEI's comments, the absence of any criticality risks or special nuclear material at uranium hexafluoride conversion facilities, and the existing cyber security programs at MTW. Our comments below are supplemental to the NEI comments and apply only to the extent that the NRC decides to proceed with the rulemaking for uranium hexafluoride conversion facilities.
7.3	Honeywell letter dated 10/2/2015 (ML15287A414)	Honeywell has two principal concerns with the draft regulatory basis beyond those articulated in the industry comments. First, Honeywell is concerned that the draft regulatory basis and the supporting analyses do not appropriately account for the existing ISA at Honeywell's Metropolis Works plant ("MTW") or explain why the ISA cannot be used as the starting point for the cyber security program. Any cybersecurity rule should focus on identifying the outcomes of a cyber attack that are most serious and applying a risk-informed approach to those outcomes to identify facility components and systems that need protection. For consistency and efficiency, the NRC should be utilizing the existing ISA for that purpose to the maximum extent possible. It makes little sense to "start from scratch" in risk informing cyber security protections when existing tools can be used to achieve the same objective more quickly and at less cost.
7.4	Honeywell letter dated 10/2/2015 (ML15287A414)	Second, the draft regulatory basis does not provide an adequate justification for imposing stringent new, stand-alone cyber security requirements on MTW given the unique hazards at a uranium hexafluoride conversion facility. The draft regulatory basis is focused primarily on risks - criticality, loss/diversion of special nuclear material, and radiological sabotage at facilities subject to the design basis threat rule - that do not exist at uranium hexafluoride conversion facilities. Rather than impose a one-size-fits-all approach for all fuel cycle facilities, the more efficient path would be to impose facility type-specific conditions, tailored to address the security posture in a site's existing security plan. It makes little sense to impose the same regulations on all fuel cycle licensees in the face of uncertain costs and even more uncertain benefits at MTW. In the end, any proposed rule must adequately account for the types of operations and low radiological risks associated with uranium hexafluoride conversion facilities.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
7.5	Honeywell letter dated 10/2/2015 (ML15287A414)	Q1: Ch 1 (pg 1-1) a) Chapter 1 of the Draft Regulatory Basis (page 1-1) describes the NRC's approach to cyber security at fuel cycle facilities as involving the following: • Require certain licensees authorize to possess a Category II or III quantity of SNM or source material to establish and maintain a cyber security program that provides reasonable assurance that digital computer systems, communication systems, and networks associated with SSEPMCA functions are protected from cyber attacks; and • Implement a "graded performance-based regulatory" framework to protect against cyber attacks that could result in a SSEPMC consequence. The overarching goal of protecting against these ultimate consequences is well intentioned, as every facility seeks to eliminate vulnerabilities associated SSEPMCA functions. But, the framework for identifying the digital computer systems, communication systems, and networks associated with SSEPMCA functions does not appear to build on existing plant knowledge and processes and instead inappropriately would require licensees to "start from scratch" in developing a cyber security program.
7.6	Honeywell letter dated 10/2/2015 (ML15287A414)	First, there is no substantive indication of what the "graded, performance-based" :framework will look like. [FOOTNOTE-2: Continued references to the "graded approach" is dealt with via statements indicating that the to-be-developed graded approach will be accompanied by "anticipated guidance."] On page 4-3 of the Draft Regulatory Basis, the NRC staff states that future guidance associated with the regulatory requirements will risk-inform the asset identification process by providing: (1) a screening methodology to account for digital assets whose equivalent SSEPMCA function may be provided by an alternate means; and (2) a graded technique to apply cyber security controls based on the level of risk associated with the SSEPMCA function for the specific facility type. Absent details on the NRC's proposed "graded, performance-based" rule and guidance, it is difficult to provide substantive comments. The details on the screening methodology and grading technique are critical to assessing the level of effort and cost associated with any rule. As a result, if the NRC proceeds with a cyber security rulemaking, it should publish the draft guidance concurrently with the proposed rule. This will permit informed comments on the proposed rule and facilitate development of an appropriate final rule.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
7.7	Honeywell letter dated 10/2/2015 (ML15287A414)	Second, and most importantly, the Draft Regulatory Basis fails to account for existing knowledge and hazard information at MTW. According to the Draft Regulatory Basis, the goal of the planned screening methodology would be to identify the initial set of digital assets (i.e., those associated with SSEPMCA functions) and refine the scope to those digital assets that would require protection under the new proposed cyber security requirements. This suggests that the "graded approach" will begin with a listing and inventory of all digital assets associated with SSEPMCA functions, followed by a screening method to determine potential consequences based on level of risk. This would then define required protection of specific digital assets. However, this approach discounts the ISA as a working tool to inform identification of the most vulnerable or critical devices. By design, the ISA identifies process controls, including administrative, engineered, passive, or active controls that are intended to reduce the likelihood of negative consequences of concern. Yet, the Draft Regulatory Basis downplays the value of the ISA, stating (at 2-7) that the "ISA is not required to consider malicious actors, nor is it required to consider any specific cyber security requirements." [FOOTNOTE – 3: The Draft Regulatory Basis does acknowledge (at 4-4) that an ISA could be used to inform cyber security requirements, but this discussion implies that the ISA is merely one tool for risk informing, rather than the starting point for any cyber security rulemaking (as Honeywell suggests).] For a system that aims to use a "graded, performance-based" approach, the ISA and subsequent safeguards - known as Plant Features and Procedures ("PFAPS") at MTW - ought to be the starting point for the assessment. While there may be other controls outside of PFAPS that will need to be evaluated, it is more efficient to "screen in" those controls than ignore the substantial work done to date in developing an ISA. Accordingly, the regulatory basis for any cyber security rulemaking ought to begin with the ISA and work out from there, rather than "start from scratch."
7.8	Honeywell letter dated 10/2/2015 (ML15287A414)	Third, the focus of the consequence-based approach to identifying assets is flawed. The Draft Regulatory Basis (at 3-8) describes the intent of the framework as protecting digital assets associated with SSEPMCA functions from cyber attacks that could result in: • A safety/security consequence of concern; or • The compromise of a function needed to prevent, mitigate, or respond to a safety/security event with the potential to cause a consequence of concern. Honeywell's primary concern is that the use of the disjunctive "or" implies that MTW must protect against any compromise of digital asset associated with a SSEPMCA function, even if a consequence will not in fact occur because of other mitigative measures. [FOOTNOTE – 4: This flawed approach is also reflected in the Draft Regulatory Basis definition of a cyber attack as "having the potential to result in a direct or indirect adverse effect or consequence to a digital asset or system." The purpose of rulemaking and cyber protection should be to protect against a safety and security consequence, not merely the compromise of a digital asset.] In developing PFAPS, there are "credits" given for safeguards leading to the characterization of a deviation as "highly unlikely" for purposes of ISA implementation. Many times, there may be more credits or additional "safeguards" available, or there may be other compensatory measures available (e.g., shut down the process or equipment). The failure of a "functional device" does not in itself necessarily result in the consequence of concern. The determination as to whether or not the consequence of concern will result from the failure of any given device will require licensees to refer back to the specific scenarios considered in the ISA. This again suggests that the ISA ought to be the starting point for the cybersecurity framework, and not a complete catalog of digital assets unmoored from pre-existing knowledge of its actual risk significance.

<table>
<tr><th>NRC #</th><th>SOURCE</th><th>STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS</th></tr>
<tr><td>7.9</td><td>Honeywell letter dated 10/2/2015 (ML15287A414)</td><td>Fourth, the Draft Regulatory Basis should more clearly and specifically acknowledge the different characteristics of uranium hexafluoride conversion facilities, which do not possess special nuclear material, from other fuel cycle facilities that may be subject to a cyber-security rule:
<table>
<tr><th>Potential Consequences</th><th>Applicable?</th><th>Comments</th></tr>
<tr><td>Nuclear criticality (safety)</td><td>No</td><td>MTW does not possess SNM.</td></tr>
<tr><td>Releases of radioactive materials or chemicals resulting in significant exposures to workers or members of the public (safety)</td><td>Yes</td><td>See below.</td></tr>
<tr><td>Loss/theft/diversion of SNM (security and MC&A)</td><td>No</td><td>MTW does not possess SNM.</td></tr>
<tr><td>Radiological sabotage (security – limited to licensees with a DBT)</td><td>No</td><td>MTW does not have a DBT.</td></tr>
<tr><td>Loss or unauthorized disclosure of classified information (security)</td><td>No</td><td>MTW does not possess classified information.</td></tr>
<tr><td>Inability to maintain onsite and offsite communications during normal and emergency operations (emergency preparedness)</td><td>Yes</td><td></td></tr>
</table></td></tr>
<tr><td>7.10</td><td>Honeywell letter dated 10/2/2015 (ML15287A414)</td><td>Honeywell has a concern with the potential consequence for safety related to releases of chemicals "resulting in significant exposures." There is no definition, or discussion, of what constitutes "significant." For example, there is no link back to performance objectives in the MTW ISA, no discussion of the maximum quantities or locations of liquid uranium hexafluoride at risk, and no assessment of whether consequences from various UF6/HF release scenarios would be considered significant. Absent such a discussion, the Draft Regulatory Basis fails to affirmatively demonstrate that the proposed approach is appropriate for uranium hexafluoride conversion facilities. The Draft Regulatory Basis must address the graded, consequence-based approach to digital asset protection specifically for uranium hexafluoride conversion facilities, in addition to applying an appropriate graded approach to the identification of digital assets based on existing risk information in the ISA (as discussed above).

Overall, a failure to clearly analyze and articulate the threat or identify the consequences of concern from a cyber attack will result in imposition of an overly broad set of requirements with a questionable regulatory basis, diverting limited resources from other safety and security activities.</td></tr>
<tr><td>7.11</td><td>Honeywell letter dated 10/2/2015 (ML15287A414)</td><td>Response to Question 2:
The NRC's approach to cyber security ought to be aligned with the NRC's historical approach and overall framework for ensuring safety at uranium hexafluoride conversion facilities. However, the Draft Regulatory Basis provides no new information to suggest that MTW is not already adequately protected and fails to conduct an integrated look at cyber security as only one aspect of site security.</td></tr>
</table>

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
7.12	Honeywell letter dated 10/2/2015 (ML15287A414)	The objective of the NRC's security regulations is that protective measures should be commensurate with the potential consequences of malevolent acts to safety and security. The scope of the Draft Regulatory Basis appears to be focused on facilities possessing material generally considered to be SNM, not natural uranium. The discussion of chemical releases, while appropriate, appears to almost be an afterthought. There is no clear linkage of the consequences of concern of facilities with SNM to a similar consequence of concern for a facility using source material (see above regarding the definition of "significant"). This is inconsistent with Commissioner Ostendorffs comments on SECY-14-0147, in which he noted that the NRC Staff should provide "a sufficient basis for the Commission to make a finding that the fuel cycle facilities regulatory functions are not currently protected in a manner sufficient to adequately protect public health and safety."
7.13	Honeywell letter dated 10/2/2015 (ML15287A414)	The introduction of a cyber attack as an adversary capability should not necessitate a substantial departure from the current security posture at MTW, which does not include a requirement to protect against a Design Basis Threat. The basis for issuing requirements to defend against cyber attacks at fuel cycle facilities that are not currently subject to the design basis threat requirements in 10 CFR 73.1 should not result in an entirely new standalone focus on cyber security. This again suggests that use of the ISA as a starting point for any cyber security program with appropriate linkages to the current site security plan, rather than an over-broad program that is not tailored to the existing security requirements for uranium hexafluoride conversion facilities.
7.14	Honeywell letter dated 10/2/2015 (ML15287A414)	In addition, the Draft Regulatory Basis does not adequately account for or acknowledge "lessons-learned" during the implementation of the cyber security requirements for power reactors. There is no discussion of any issues that arose during initial implementation of a cyber-security rule for reactors or that are currently the subject of discussions between the NRC and Part 50 licensees, such as the need to closely align consequences with the scope of assets being protected. Incorporating lessons-learned is a hallmark of the U.S. nuclear industry. Yet, the draft regulatory basis documents do not explicitly consider improvements or enhancements based on the Part 50 experience. Lessons learned must be applied to avoid undue burden to both NRC and industry in this regulatory initiative.
7.15	Honeywell letter dated 10/2/2015 (ML15287A414)	Response to Question 3: The Draft Regulatory Basis is wholly inadequate in its discussion of cost impacts. There is simply no basis provided for the statement that the costs associated with a cyber security rulemaking will be "offset" by preventing cyber attacks that could result in potential consequences. This is especially the case for MTW, as only two of the six potential consequences implicate uranium hexafluoride conversion facilities (there is no SNM, no DBT, and no classified information at MTW). Given that several of the most serious concerns supposedly addressed by the cyber security regulatory basis (criticality, loss/theft/diversion of SNM, and radiological sabotage) are inapplicable to MTW, the NRC must develop a specific cost justification for uranium hexafluoride conversion facilities. There is no rational basis for applying the same cost-benefit analysis to MTW as for Category I, II, and III facilities that possess SNM.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
7.16	Honeywell letter dated 10/2/2015 (ML15287A414)	Response to Question 3: In addition, the Draft Regulatory Basis again fails to consider the existing information available as part of the plant ISA. The ISA process looks at failure mechanisms and develops safeguards so that that an event of significance is "highly unlikely." In this analysis, failure of individual devices is considered and compensatory measures developed. While cyber attacks are not a specific initiating event, the failure of a device (for any reason) is considered in developing the ISA. This would suggest that the incremental benefit of evaluating cyber "failure" will add little to no value, as the analysis has already considered the failure of individual devices.
7.17	Honeywell letter dated 10/2/2015 (ML15287A414)	Response to Question 3: Finally, because the Draft Regulatory Basis does not establish the scope of the program, except to refer to future implementation of a graded approach, it is impossible to make an assessment of a "reasonable cost estimate for implementation ... startup and annual costs." Nevertheless, assuming that the assessment framework uses the "wide net" approach implied by the Draft Regulatory Basis to capture the universe of digital control assets subject to the cyber security program, we estimate that the initial implementation costs at MTW could exceed $17 million, including costs for inventory of devices, classification of consequences, assessments by expert team, and final disposition. This cost is wholly disproportionate to the benefits of a cyber security rule - particularly in light of the absence of an adequate discussion of the need for such a program given the existing ISA and security measures already in place. As an additional data point, should the NRC decide to base the scoping framework on the existing ISA, the cost of initial implementation could fall within the $1-$2 million range. While less costly, even the lower cost estimate is a substantial sum for little demonstrated benefit.
7.18	Honeywell letter dated 10/2/2015 (ML15287A414)	Response to Question 4: Honeywell has spent, and will continue to spend, significant resources on implementing cyber security programs. Honeywell has already adopted four voluntary initiatives to reduce the risk of a cyber attack at MTW. These initiatives include (1) forming a cyber team; (2) providing technical cyber training to the cyber team and general training to plant workers; (3) implementing mobile controls (e.g., for portable media and devices); and (4) providing incident detection and response. However, there are other existing processes and analyses that must be considered when developing the regulatory basis for any cyber security rulemaking. For example, Honeywell has voluntarily submitted an ISA, which is part of the licensing basis for MTW. The ISA already has identified and maintains process controls that are intended to reduce the likelihood of negative consequences of concern. In developing PF APS, there are "credits" given for safeguards leading to the characterization of a deviation as "highly unlikely" for purposes of ISA implementation. There may be more credits or "safeguards" available, or there may be other compensatory measures available that would prevent a consequence even if digital assets were compromised. The determination as to whether or not the consequence of concern will result from the failure of any given device as a result of a cyber attack necessarily will require licensees to refer back to the specific scenarios considered in the ISA. As a result, the NRC should be using the ISA as the starting point for the cybersecurity framework in order to take advantage of existing assessments of hazards and minimize unnecessary costs associated with any new cyber security rulemaking.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
7.19	Honeywell letter dated 10/2/2015 (ML15287A414)	In Chapter 6 of the Draft Regulatory Basis, the NRC notes that there is not currently a backfit provision in 10 CFR Part 40. However, in a recently-terminated Part 40 rulemaking, the NRC Staff had, at the Commission's direction, proposed a backfit provision for Part 40 licensees. See, e.g., "Domestic Licensing of Source Material-Amendments/Integrated Safety Analysis," 76 Fed. Reg. 28336 (May 17, 2011). The decision to terminate the rulemaking was unrelated to the backfit provision. Moreover, NRC regulations applicable to power reactors, gaseous diffusion plants, Part 70 licensees (fuel fabricators and uranium enrichment facilities), and independent spent fuel storage facilities contain backfitting provisions at 10 C.F.R. §§ 50.109, 76.76, 70.76, and 72.62, respectively. 5 As the Commission has noted, backfit management is of paramount importance to responsible regulatory practice. 50 Fed. Reg. at 38104. The backfit rule as applied to other NRC licensees is intended to provide for a formal, systematic, and disciplined review of new or changed NRC positions before imposing them on licensees. Discipline and management of backfitting ensure that attention and priorities are focused on areas where action is justified to carry out the NRC's regulatory responsibilities.
7.20	Honeywell letter dated 10/2/2015 (ML15287A414)	In light of the above, Honeywell strongly urges the NRC to conduct the equivalent of a backfit analysis for any cyber security rulemaking that applies to uranium hexafluoride conversion facilities. Such an analysis is vital to ensure that a formal, systematic, and disciplined review of plant modifications imposed by any cyber security rule will improve the overall effectiveness and certainty in the regulatory process, thus enhancing the NRC's regulatory mission.
7.21	Honeywell letter dated 10/2/2015 (ML15287A414)	Honeywell appreciates the NRC's stated goal ofrisk informing decisions on which digital assets are of concern. However, the Commission and the Obama administration both have expressed a strong interest in providing greater predictability and transparency to regulatory activities. The Draft Regulatory Basis is inconsistent with this objective. The Draft Regulatory Basis does not provide a sound risk and performance-based foundation for a cyber security rulemaking. Nor does it promote predictability, reduce uncertainty, or identify and use the best, most innovative, and least burdensome tools for achieving regulatory ends.
8.1	CB&I AREVA MOX Services letter dated 10/5/2015 (ML15287A417)	Include the following exemption for the application of this regulation: “Any digital asset residing within an accreditation boundary Certified and Accredited under another agency's (DOE, NNSA, etc.) 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, etc.).” The regulatory basis already includes an exemption for classified systems accredited by other agencies, presumably 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.
8.2	CB&I AREVA MOX Services letter dated 10/5/2015 (ML15287A417)	Since the list of digital assets that perform functions that could result in consequences of concern are well understood, consider starting with this subset of licensee digital assets rather than requiring the licensee to tabulate thousands of SSEPMCA digital assets for which no critical safety or security function has been identified.
8.3	CB&I AREVA MOX Services letter dated 10/5/2015 (ML15287A417)	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 space (ISA) and security space (DBT and VA).

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
8.4	CB&I AREVA MOX Services letter dated 10/5/2015 (ML15287A417)	CB&I AREVA MOX endorses the use of the national consensus standard for cyber, NIST 800 series, as the basis for an NRC cyber program.
9.1	NFS letter dated 10/5/2015 (ML15292A559)	Nuclear Fuel Services, Inc. (NFS} fully endorses the letter submitted by the Nuclear Energy Institute (NEI) on October 5, 2015, (Reference 1) regarding the Nuclear Regulatory Commission's (NRC's) Fuel Cycle Facility Cyber Security Draft Regulatory Basis (80 FR 53478), NRG Docket 2015-0179, issued on September 4, 2015, (Reference 2). NFS would like to take this opportunity to support the NEI letter which incorporates feedback from NFS in the industry comments attachments. BWX Technologies Nuclear Operations Group-Lynchburg (BWXT NOG-L) hosted an NRG Cyber Security team visit to review the status of cyber security voluntary action implementation. NFS (a BWX Technologies company) was in attendance for the review which occurred the week of September 28, 2015, and provided the NRC team a description of similarities and differences between the NFS and NOG-L facilities. It is NFS' intent to continue working with the NRG to improve overall Cyber Security and protect critical infrastructure by actively participating in the rulemaking process.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
10.1	URENCO letter dated 10/5/2015 (ML15287A412)	The NRC has released a proposed rulemaking regulatory draft basis document with regard to the Cyber Security posture of network and computer systems that are associated with Safety, Security (physical and information), Emergency Preparedness (to include offsite communications), and Material Control and Accountability (SSEPMCA) functions. To UUSA this would have an impact on the way the business performs and applies security control mechanisms to various systems, specifically, the proposed rule would affect: systems utilized by Emergency Preparedness (EP) (both contracted and UUSA operated) in their operations center and at the training center in Eunice; SAP which is utilized for Material Control and Accountability; the security and access control systems; fire detection systems; and criticality alert systems. Some of these systems, specifically SAP and those utilized by EP, are a part of UUSA's privately owned business network. As such, the aforementioned systems would require the development of an Information Security Plan to be reviewed and approved by the Nuclear Regulatory Commission (NRC). Background: In 2002 the Government passed what is known as the E-Government act. Title III of the law contains provisions known as the Federal Information Security Management Act (FISMA). The purpose of this law was to address and standardize the way in which the Federal Government agencies protect information within Federal information processing systems. FISMA directed all Government agencies to apply the framework provided by the National Institute of Standards and Technology (NIST) in the development and implementation of their networks and computer information systems. This was to allow for a standardized process, thus enabling efficiency and cost savings by allowing systems developed by one agency to easily be adopted and implemented by other agencies without having to re-accomplish the entire process from the start. The result however has been questioned by many throughout the security community. Security experts from the SANS Institute have described FISMA as simply replacing one paperwork drill for another and have criticized that the framework measures security planning and not actual information security. A former Government Accountability Office (GAO) chief Page 1 of 5 technologist, Keith Rhodes has cautioned that "implementation is everything. If security people view FISMA as just a checklist, nothing is going to get done." Comments on Chapter 1: The Draft Regulatory Basis Document proposes to codify, in regulatory actions that must be taken to protect against Cyber Security threats. Please note that the systems in question (SSEPMCA systems) are privately owned (UUSA) and not a government organization, and as such, they are not Federal Information Systems. 800 series documents produced by NIST state the following in the "Authority" section in the beginning of the document directly after the title page: "This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST".

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
10.2	URENCO letter dated 10/5/2015 (ML15287A412)	Comments on Chapter 1: (continued) Within Chapter 1 the NRC defines a cyber-attack with a very broad definition: "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 direct or indirect adverse effects or consequences to digital assets or systems." This broad definition is not conducive to the protection of information or the system on which information is contained. We understand that this definition is consistent with Regulatory Guide 5.71 developed for power reactors; but with the lessons learned discussed in the NRC Public Meeting on September 23, 2015 and as stated in Section 3.3 of the draft regulatory basis document, this guidance is not appropriate to address the unique programs' associated risks specific to Fuel Cycle Facility licensees. Ultimately, this definition is the foundation of this proposed rule. Utilizing the definition above, one could come to the conclusion that an individual who simply turned the computer off at the end of the day, preventing it from receiving updates, is guilty of a cyber attack. Another example is an employee who watches an instructional video as part of training and the result is a degradation of network resources and bandwidth. While certainly there are events which occur within network systems that may have a negative effect, not all events are attacks. An attack is targeted or directed in nature and is generally related to offensive nature and malicious intent. UUSA recommends this definition be revised to reflect the actual defined threat that the NRC intends to defend against and not encompass events that could possibly occur on a computer system.
10.3	URENCO letter dated 10/5/2015 (ML15287A412)	Comment on Chapter 2: The draft rulemaking document suggests the implementation of controls provided by NIST Special Publication (SP) 800-53, Rev 4, Recommended Security Controls for Federal Information Systems and Organizations. NIST SP 800-53 Rev 4 is simply a catalog of controls Page 2 of 5 that can be applied to information systems. This document does not provide a holistic approach to the implementation of a process in which to apply those controls, nor does it define any roles, responsibilities, or expectations. The document that lays the actual framework for the implementation of the security controls is NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, and NIST 800-39, Managing Information Security Risk. The problem with the approach of the draft regulatory basis document is that it points to NIST SP 800-53 Rev 4 but it does not provide a framework or process for its implementation. Within NIST 800-53 there are over 1600 individual points (when all controls, and control enhancements are thoroughly addressed) of interest that could be addressed within a Systems Security Plan. IT security is a process, not simply the application of controls and a documentation effort. There are roles and responsibilities that prevent conflicts of interest and establish the formal acceptance of risk. The systems the NRC is wanting to regulate with this proposal are business systems. This means that the Government is not the Authorizing Official as defined within the NIST Risk Management Framework. The operation of these systems is a business risk accepted and authorized by UUSA management.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
10.4	URENCO letter dated 10/5/2015 (ML15287A412)	Comment on Chapter 2: (continued) The risk based decision to operate an IT system and the supporting processes is subjective; it is related to multiple factors ranging from risk appetite to financial considerations. We recommend having an objective basis in order to avoid differences in opinion on the subjective decision making factors currently written in the draft.
10.5	URENCO letter dated 10/5/2015 (ML15287A412)	Comments on Chapter 3: The risk based approach to the application of security controls intends to address three areas of concern, known in the community as the security triad. These areas of concern are Confidentiality, Integrity, and Availability. Confidentiality concerns itself with the inability of data to be intercepted and read by unauthorized individuals. Integrity refers to the accuracy of data being interpreted by the user and ensuring that data is not modified in an unauthorized and potentially malicious manner. Availability is the system's ability to withstand attack or other service interruptions by incorporating failsafe, redundant design. With these three pillars of protection in mind it is can be said that the goal of a successful IT security program is providing the right data, to the right people, at the right time. Each of these areas of concern (Confidentiality, Integrity, Availability) is rated as either a High, Moderate, or Low level of concern. This final rating dictates the amount of controls that are recommended as applicable from NIST 800-53. Chapter 3 of the draft document aims to address each of the SSEPMCA yet fails to adequately describe the level of concern for each system supporting it's respective SSEPMCA function. Most all functions contained in the sections of this chapter utilize general statements like the following: "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 function." This language implies that confidentiality and integrity is not a high level of concern and the focus seems to be on availability. Considering that our classified systems have been rated at "Moderate, Low, Low" levels of concern for "Confidentiality, Integrity, and Availability" respectively, NIST 800-39, Managing Information Security Risk, recommends that a Risk Assessment be performed. This would also fall in compliance with NIST 800-30, Guide for Conducting Risk Assessments. This would provide an accurate categorization of the systems in question.
10.6	URENCO letter dated 10/5/2015 (ML15287A412)	Comment on Chapter 4: Cyber vulnerabilities have not been established in this draft Regulatory Basis Document. The NRC has not shown in the draft nor in other documents that the industry has a problem. In fact, many of the systems identified have been scrutinized by the NRC and DOE, and to date no issue has been identified. Therefore, it is unclear as to why the NRC would regulate a business network that seems to be outside of the regulatory purview.
10.7	URENCO letter dated 10/5/2015 (ML15287A412)	Comment on Chapter 4: (continued) It is conventional for licensees to assume the risk for Confidentiality, Integrity, and Availability (NIST 800-53). The NIST standard leaves an interpretation that the NRC is going to assume the risk for areas which are part of a government business process. It seems as though the intention is not applicable for private business processes that has no impact on safety or security. This is strictly a business and primarily financial risk.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
10.8	URENCO letter dated 10/5/2015 (ML15287A412)	Comment on Chapter 8: (continued) Cost considerations for the proposed rulemaking as currently written, could be very broad due to the fact that many of the considerations would include the additional head count to security organizations from IT Security people to an IT Network Administrator. The man hours associated with a system that is NIST 800-53 compliant has a lot of parts that have to be verified on a regular basis. (Logs, Access, scanning of software and monitoring of systems). The cost of maintenance of the systems could also go up due to strict configuration management processes that would have to be in place to ensure compliance with NIST standards.
10.9	URENCO letter dated 10/5/2015 (ML15287A412)	The Draft Regulatory Basis document seems to be very broad and it does not seem appropriate for all fuel cycle facilities. There is still a question to the fact that NRC has not provided information to an actual threat of these systems and how they relate to the safety of a plant and community. It is unclear whether NRC intends to provide clear set of standards in order to better identify which assets within a network centric environment are not owned or operated by the Government.
10.10	URENCO letter dated 10/5/2015 (ML15287A412)	Summary: The Draft Regulatory Basis Document, Rulemaking for Cyber Security at Fuel Cycle Facilities, seems to be very broad and it does not seem appropriate for all fuel cycle facilities. The implementation of the risk based approach to fuel cycle facilities (NIST 800-53) would have a greater impact on the business systems than safety and security systems due to the majority of the licensees geographically not being in the same location. What has not been established is the basis for which the NRC will be regulating business related networks or systems that have no impact on safety or security. The implementation of a risk based approach involves a great deal with NRC providing threat and vulnerability information and how this will be established for each licensee. There still is a question to the fact that NRC has not provided information to an actual threat to these systems and how they relate to the safety of a plant and community. With a risk based approach provided by NIST, which seems to be focused on continuous improvement and monitoring; how does the NRC intend to fit the Risk Management Framework into a performance-based model of regulation? Performance-based contract models generally employ the tracking of implementation times and percentages of completion in order to produce quantifiable data in which to grade performance. It is unclear whether the NRC intends to provide clear set of standards in order to better identify which assets within a network centric environment are not owned or operated by the Government.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
11.1	Westinghouse letter dated 10/5/2015 (ML15287A415)	Westinghouse has two overarching concerns with the draft Regulatory Basis document. Broad Scoping Language First, the scope of digital assets that would be subject to NRC cyber security requirements is unclear. Westinghouse has concerns with the NRC's approach to use broad language in the rule (similar to the existing language in 1OCFR73 .54 for power reactors), with the specific criteria for consequences of concern in regulatory guidance. Additionally, the recently issued Part 73 Regulatory Basis Document states that "the new structure places the requirements in regulation rather than partially addressing these areas in regulatory guidance. This approach is consistent with NRC 's policy that regulatory guides should, in part, describe acceptable ways to meet the regulations and should not impose requirements beyond those in the regulations." [Regulatory Basis Document for Rulemaking for Enhanced Security of Special Nuclear Material, page 35]. In contrast, the cyber security draft Regulatory Basis also in Part 73 regulations does not provide an appropriate level of detail to understand the consequences of concern by facility type. Instead, the consequences are defined in general terms with the intent of clarifying the details in regulatory guidance. Without providing this level of detail, it is difficult for Westinghouse to accurately assess the impact of proposed NRC cyber security requirements. We believe proper specification of the consequences of concern in the rule could address these scope concerns.
11.2	Westinghouse letter dated 10/5/2015 (ML15287A415)	Westinghouse understands that the staff has identified a regulatory gap. We believe the staff should tie each proposed requirement to the identified gap and describe how the requirement contributes to closing the gap. As written, the draft Regulatory Basis applies to the full range of FCFs and mixes the bases for the various categories of licensees together. The resulting conclusion that regulatory action is needed for each category of licensee may not be valid when each is looked at separately. Additionally, the draft Regulatory Basis focuses in many areas on preventing a cyber attack or protecting digital assets rather than preventing a consequence of concern to public health and safety or common defense and security.
11.3	Westinghouse letter dated 10/5/2015 (ML15287A415)	It is Westinghouse's view that the draft Regulatory Basis goes significantly beyond what is necessary to meet the intent of the Commission's direction, namely, to prevent consequences of concern. [SRM-SECY-14-0147] Specifically, the staff is focused on preventing degradation of “junctions” as opposed to preventing events with clear performance objectives. This approach will dramatically and unnecessarily increase the scope and cost of implementation of any Rule that is derived from a regulatory basis similar to this draft. Westinghouse believes in a risk-informed and consequence-based approach to Rulemaking that is "commensurate with the inherent nuclear safety and security risks associated with the different types of licensees and facilities" [Draft Regulatory Basis Document for Rulemaking for Cyber Security at Fuel Cycle Facilities, page 2-2] and based on the "specific operational characteristics and potential consequences" of FCF licensees [Draft Regulatory Basis Document for Rulemaking for Cyber Security at Fuel Cycle Facilities, page 4-2].

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
11.4	Westinghouse letter dated 10/5/2015 (ML15287A415)	The second concern is that, as written, the draft Regulatory Basis introduces Policy issues which are discussed only superficially. For example, the draft Regulatory Basis identifies that "[t]he ISA is not required to consider malicious actors." [Draft Regulatory Basis Document for Rulemaking for Cyber Security at Fuel Cycle Facilities, page 2-7] It is unclear how a Category III facility, such as the CFFF, should assess a malevolent actor. Also, the staff does not make a case as to why protections against cyber sabotage are needed, despite no requirement for physical sabotage protections at a Category III FCF. Based on the draft Regulatory Basis, cyber security for Category III FCFs appears to have a special emphasis as compared to physical security requirements. In the recently issued Part 73 Regulatory Basis Document, NRC reassessed the physical security requirements for Special Nuclear Material (SNM). This approach developed protection strategies that are informed by current threat intelligence and the material attractiveness of the SNM. This document concluded that no increase in physical protection was needed for facilities with Category III SNM, enriched to less than 10 weight percent U-235. NRC also determined that there is no increased sabotage risk for these facilities and that no additional protection was needed to manage the risk of an insider threat. 7 In contrast, it is not clear how the cyber security draft Regulatory Basis considers these risk insights and in fact actually applies more cyber security protections to SNM than currently exist for physical protection.
11.5	Westinghouse letter dated 10/5/2015 (ML15287A415)	Specific comments supporting these concerns are enclosed in Attachment 1 of this letter. Westinghouse also endorses the detailed comments that the Nuclear Energy Institute (NEI) provided on behalf of its FCF members. We are eager to see the proposed resolution of these and other comments received on the draft Regulatory Basis. Resolution of the comments and their availability to the public and/or licensees is a critical interaction between the stakeholders and NRC. Attachment 1: Broad Definition of Cyber Attack and Identifying the Consequences of Concern in line with the NRC mission to "protect people and the environment', the Cyber Security Rulemaking should focus on the protection against clear performance objectives and not on the protection of digital assets. Instead the draft Regulatory Basis focuses on preventing a cyber attack, using the definition: "[having] the potential to result in a direct or indirect adverse effects or consequences to a digital asset or system" [Draft Regulatory Basis Document for Rulemaking for Cyber Security at Fuel Cycle Facilities, page 1-1] rather than protecting from the consequences of a cyber attack. Westinghouse believes that the consequence of concern for the Rulemaking should start with cyber events that may result in a high or intermediate consequence per the performance objectives in 10 CFR 70.61. The consequences in 70.61 already exist in the regulation for FCFs and are well understood by the NRC and industry. It is unclear why new consequences need to be created specifically for this rulemaking. Additionally, the consequence of concern should exclude the Safeguards disciplines (Physical Security+ Material Control & Accounting) for a Category III facility, such as the CFFF, for reasons discussed in the policy section of the cover letter to this attachment. Emergency Planning should be excluded as well due to the FCF's ability to perform these functions, even with the compromise of a digital asset.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
11.6	Westinghouse letter dated 10/5/2015 (ML15287A415)	The NRC staff believes that the "cyber security initiative should address cyber attacks that could compromise items relied on for safety (IROFS), rendering them unavailable or unreliable to protect against potentially high and some intermediate consequences, both on and off-site." [SECY-14-0147, Enclosure 1, page 2] However, this approach does not consider potential redundant controls (e.g., multiple IROFS) that may be in place to prevent or mitigate accident consequences. The NRC staff agrees that if an "equivalent function" can be shown, then cyber security requirements should be not placed on the original digital asset. [SECY-14-0147, Enclosure 2, page 5] Westinghouse agrees with the ability to credit redundant and/or multiple IROFS, which is also consistent with the performance requirements in 10 CFR 70.61. Westinghouse does not believe that degraded IROFS should be classified as a consequence of concern within the scope of a cyber security rule.
11.7	Westinghouse letter dated 10/5/2015 (ML15287A415)	Westinghouse agrees that the ISA should be used to identify scenarios which can lead to high or intermediate consequence events and rely solely on digital assets, such as active engineered controls or augmented administrative controls. These are then reviewed to determine those scenarios that have digital asset vulnerabilities with no redundant or alternative controls. This approach uses a screening methodology, similar to what industry proposed in October 2013. Performing a baseline assessment of all digital assets on site is an unnecessary burden expected to produce little safety benefit and does not align with the "disciplined, graded approach to the identification of digital assets." [SRM-SECY-14-0147]
11.8	Westinghouse letter dated 10/5/2015 (ML15287A415)	Because there is variability in the scope defined for the Cyber Security Rulemaking and because many of the measures described in the draft Regulatory Basis are conceptual and open for interpretation, cost estimates are difficult to provide. However, below we outline order of magnitude cost estimates with supporting assumptions. Scenario 1: If the consequence-based risk-informed approach is used, we estimate it will cost on the order of $10-$15 million through 2019. Assumptions: Consequence-based and risk-informed Rulemaking with clearly defined scope Close alignment with "voluntary actions" licensees are currently taking. Scenario 2: If the scope of Rulemaking includes all digital and protects their functions, we estimate it could double the cost and significantly increase the implementation period. Assumptions: Baseline development of all digital assets as starting point for initial assessment Vulnerability assessment for cyber attack Extension application of NIST SP 800-53, Revision 4 controls. Given the order of magnitude cost values presented in this Attachment, Westinghouse believes that the imposition of new cyber security requirements must be justified through a cost benefit analysis to assure that there is a safety and security benefit commensurate with the risks the CFFF presents to the public, its employees, or the environment.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
11.9	Westinghouse letter dated 10/5/2015 (ML15287A415)	During the May 19th Commission Briefing on Cumulative Effects of Regulation (CER) and Risk Prioritization Initiatives, the key message embraced by NRC staff, industry, and other external panel members was that industry and NRC limited resources should be applied to the most safety significant activities. [Transcript of May 19, 2015 Commission Briefing on Update on Cumulative Effects of Regulation and Risk Prioritization Initiatives] Westinghouse is in full alignment with that view, and that philosophy guided our feedback on Project Aim 2020 and is summarized, with emphasis on Part 70 activities, below. [LTR-NRC-15-74, September 14, 2015, Westinghouse (Weaver) letter to NRC (Brown)] Given the Cyber Security activities for FCFs started in 2011 with the cyber security working group, planned a rulemaking in 2012, visited sites in 2013, proposed orders in 2014 [SECY-14-0147, pages 3-5, 9] , and finally, started a rulemaking in 2015, there have been many staff resources applied to the topic of Cyber Security for FCFs. SRM-SECY-14-0147 directed the staff to pursue rulemaking instead of issuing Cyber Security Orders, with Commissioner Ostendorff noting "a sufficient basis" has not been provided to show that FCFs "are not currently protected in a manner sufficient to adequately protect public health and safety and the common defense and security." [Commissioner Ostendorff's Notation Vote sheet for SECY-14-0147] Considering the resources spent to date on this effort and Issue R-1 from the Project Aim 2020 feedback letter [LTR-NRC-15-74, September 14, 2015, Westinghouse (Weaver) letter to NRC (Brown)], Westinghouse encourages the staff to produce a more robust regulatory basis early in the rulemaking process to determine the anticipated safety benefit and determine if it is more or less beneficial than activities licensees are voluntarily taking.
11.10	Westinghouse letter dated 10/5/2015 (ML15287A415)	In addition to rulemaking activities, Westinghouse suggested the following activities, as related to the CFFF should be terminated because they do not have a demonstrated safety benefit: 1. The rulemaking to clarify requirements in Part 21, Reporting of Defects and Noncompliance should be terminated and the resources re-assigned to review the proposed industry guidance. The rulemaking has little or no safety benefit as articulated in our letter, LTR-NRC-15-51, dated June 18, 2015. To the extent that clarity is needed, NRC should instead focus on reviewing and providing feedback on the NEI draft guidance (NEI-14-09) that was submitted for review in August 2014. For facilities licensed under Part 70, this rulemaking has no safety benefit, and in fact could be detrimental to safety due to unintended consequences.
11.11	Westinghouse letter dated 10/5/2015 (ML15287A415)	2. Efforts to develop quantitative dermal and ocular exposure standards for workers should be terminated, as expressed in our letter LTR-RAC-15-36 dated June 30, 2015. NEI and industry correspondence over the past several years has amply demonstrated that this initiative yields no safety benefit. NRC staff has also stated there is no safety issue and therefore the staff should close this issue.
11.12	Westinghouse letter dated 10/5/2015 (ML15287A415)	3. The Part 73 rulemaking for enhanced security for SNM should be terminated. There is no sound or justifiable regulatory basis for new or modified requirements.
11.13	Westinghouse letter dated 10/5/2015 (ML15287A415)	4. The Part 73 rulemaking for amending material control and accounting regulations should be terminated. The rule language is ambiguous and there is the potential to impose significant new burden with little to no improvement to safety.

NRC #	SOURCE	STAKEHOLDER COMMENT ON THE DRAFT REGULATORY BASIS
11.14	Westinghouse letter dated 10/5/2015 (ML15287A415)	5. Efforts to create an Integrated Safety Analysis Standard should be terminated. There is no value in creating a standard when a clear regulation and guidance already exist.