Section III and Section IV of the Federal Register Notice publishing the draft Regulatory Basis for cyber security for fuel cycle facilities requested that stakeholders consider specific questions on the draft Regulatory Basis and Cumulative Effects of Regulation. This attachment provides feedback to those specific questions.

Question Section III-1:

Is the NRC considering an appropriate approach for each objective described in the draft regulatory basis?

Chapter 1, "Introduction and Background" of the draft regulatory basis lists six specific objectives. Each bullet below addresses the approach for each objective.

- *Objective: require licensees authorized to possess a Category I quantity of special nuclear material (SNM) to establish and maintain a cyber security program that provides high assurance that digital computer systems, communication systems, and networks associated with safety, security (physical and information), emergency preparedness (to include offsite communications), and material control and accountability (SSEPMCA) functions are protected from cyber attacks up to and including the design basis threats (DBTs) as described in 10 CFR 73.1*.

  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.

  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.

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.

- *Objective: require certain licensees authorized 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.*

  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 UF_6 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.

  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. The cost considerations in the draft regulatory basis provide no cost estimates or justification that the expected implementation cost is justified by the risks. 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.

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.

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.

- *Objective: codify in regulations existing cyber security requirements imposed on FCF licensees by security orders issued following the terrorist attacks of September 11, 2001.*

  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.

- *Objective: codify in regulations voluntary cyber security actions instituted by FCF licensees.*

  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.

- *Objective: implement a graded, performance-based regulatory framework to protect against cyber attacks at FCFs that could result in SSEPMCA consequences .*

  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.

- *Objective: implement cyber security reporting criteria.* It appears unnecessary for this objective to be addressed in a rulemaking.

  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.

Question Section III-2:

Chapter 3 of the draft regulatory basis discusses the regulatory concerns the NRC expects to address through rulemaking. Chapter 4 presents the intended regulatory changes to address those regulatory concerns, and Chapter 5 discusses alternatives to rulemaking considered by the NRC staff. Are there other regulatory concerns within or related to the scope of the rulemaking efforts (see Chapter 1 of the draft regulatory basis) that the NRC should consider? Are there other approaches or alternatives the NRC should consider to resolve those regulatory concerns?

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.

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.

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.

Question Section III-3:

Chapter 8 of the draft regulatory basis presents the NRC staff's initial consideration of costs and other impacts for a number of key aspects of the potential regulatory changes (i.e., cyber security programs, cyber incident reporting). This initial assessment is based on limited available data. The staff is seeking additional data and input relative to expected and/or unintentional impacts from the desired regulatory changes. What would be the potential impacts to stakeholders/licensees from implementing any of the desired regulatory changes described in this draft regulatory basis (e.g., what would be a reasonable cost estimate for implementation of the cyber security programs, including startup and annual costs)?

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.

Question Section III-4:

The NRC staff is aware of licensee voluntary efforts to address cyber security. Is there additional information related to these efforts that would inform the NRC staff's assessment or analysis?

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.

Question Section IV-1:

In light of any current or projected CER challenges, what should be a reasonable effective date, compliance date, or submittal date(s) from the time the final rule is published to the actual implementation of any new proposed requirements, including changes to programs, procedures, or the facility?

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.

Question Section IV-2:

If current or projected CER challenges exist, what should be done to address this situation (*e.g.,* if more time is required to implement the new requirements, what period of time would be sufficient, and why such a time frame is necessary)?

To address CER challenges, NRC should move quickly to implement the Commission's direction on Project AIM and use industry's feedback[1] 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.

Question Section IV-3:

Do other regulatory actions (*e.g.,* orders, generic communications, license amendment requests, and inspection findings of a generic nature) by NRC or other agencies influence the implementation of the potential proposed requirements?

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.

[1] September 15, 2015, John Butler (NEI) to Frederick Brown (NRC); Industry Recommendations for NRC Project AIM 2020 Prioritization and Re-baselining Initiatives

Question Section IV-4:

Are there unintended consequences? Does the potential proposed action create conditions that would be contrary to the potential proposed action's purpose and objectives? If so, what are the consequences and how should they be addressed?

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.

Question Section IV-5:

Please provide information on the costs and benefits of the potential proposed action. This information will be used to support any regulatory analysis by the NRC.

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.