PUBLIC MEETING SUMMARY REGARDING THE PROPOSED CYBER SECURITY RULEMAKING AT FUEL CYCLE FACILITIES
March 17, 2016

On March 17, 2016, the U.S. Nuclear Regulatory Commission (NRC) staff held a public meeting in Atlanta, Georgia to discuss concepts for the proposed cyber security rulemaking for fuel cycle facilities. The presentation included four discussion areas including: proposed rulemaking status, insights from implementation of Title 10 of the *Code of Federal Regulations* (10 CFR) Section 73.54, identification of digital assets within scope, and application of adequate controls. The summary below represents an overview of the discussions held during the meeting and does not necessarily represent the NRC's final policy on the issues.

Session 1 – Proposed Rulemaking Status:

The NRC staff provided an update on the proposed rulemaking timeline. The points highlighted included completion of the regulatory basis in March 2016. The next opportunity for public interaction is scheduled for December 2016 when the proposed rulemaking is published for comment. Industry requested the NRC staff consider additional opportunities for meeting on the draft proposed rule concepts, prior to submission to the Commission. Additional opportunity for meetings would provide opportunity for the NRC staff to publish draft rule language and guidance in order to receive feedback. Additional public meetings would require extending the proposed rulemaking timeline.

The draft proposed rulemaking concepts were presented along with a summary of the feedback received during the previous public meeting on February 18, 2016. Additional stakeholder feedback was requested. An individual requested clarification on whether the scope of the rulemaking would include both digital and non-digital assets. Only digital assets are within scope for this rulemaking. Stakeholder input on the draft proposed rule language will be considered in the development for the proposed rule package and related guidance.

Session 2 – Insights from Implementation of 10 CFR 73.54:

The NRC staff presented the major insights gained from implementation of 10 CFR 73.54 that have been incorporated into the fuel cycle cyber security proposed rulemaking. The proposed rulemaking seeks to implement a risk management framework rather than a prescriptive list of controls. Licensees would be required to conduct an analysis to identify digital assets susceptible to a cyber attack that could result in a consequence of concern. Once these digital assets are identified, licensees would implement a risk-informed screening process to identify and credit alternate controls available to prevent the consequence of concern. If additional controls are necessary, licensees would be able to tailor the baseline set of controls based on plant conditions. The timeframe to implement the rule, if approved, would have established deadlines.

An individual asked if the NRC staff intends to publish the guidance at the same time as the rule language, which is the NRC's plan. The individual indicated that a lesson learned from 10 CFR 73.54 was that early opportunities to review and comment on the guidance, even early drafts, improved the overall product and led to better industry understanding of the NRC staff's approach for the proposed rule. Another individual stated that a firm deadline for implementation was beneficial, but requested the NRC consider several phases of

implementation with time to remediated deficiencies between each phase. An individual asked if the NRC planned to incorporate any lessons learned from the petition for rulemaking to 10 CFR 73.18. The NRC staff indicated that the rulemaking would need be finalized before any lessons learned could be incorporated.

Several individuals asked if the NRC could gain any lessons learned from the cost estimates conducted for the 10 CFR 73.54 rulemaking. The NRC plans to seek insights from the costs expended to implement cyber security at the NRC and other Federal agencies. The individual expressed concern that the controls implemented at fuel cycle facilities would be dramatically different than those implemented by Federal agencies. Costs for implementing 10 CFR 73.54 at the reactor facilities may be more relevant for estimating costs for industry.

Several individuals asked if the cyber security plan would need to be submitted to the NRC for review and approval. The cyber security plan would be similar to the licensees existing security plans and would require submittal to the NRC for approval. One individual asked what the inspections would review. The inspections would evaluate the implementation of the approved cyber security plan.

Several questions were raised regarding how risk would be used to determine the scope of digital assets that need to be protected. One individual asked how licensees would accept residual risk and also demonstrate adequate protection. Another individual asked if the NRC plans to define the minimum level of risk that must be protected against to comply with the performance objectives. A commenter expressed concern that the NRC staff and licensees may disagree on the level of risk that could be accepted. One individual asked the NRC to clearly define the type of malicious actor, their capabilities, and the threat. Another individual indicated the NRC should notify licensees in the event of credible threat intelligence. The NRC indicated that it has several tools at its disposal to inform licensees and direct additional protective actions when needed. These include advisories, generic communications, and orders.

Some members of industry questioned the need for the authorizing official and the independent assessment. Licensees indicated they should be allowed to use expert staff in the cyber security teams to identify deficiencies, address them through some form of corrective action programs, seek management buy-in for changes, and work toward resolution. Licensees already implement audits which should take the place of the independent assessment. They proposed that the cyber security program should be implemented with a structure (e.g., a team of experts to run the program, management oversight, regular audits, some form of corrective action program, etc.) similar to other regulatory required programs (e.g., security; material, control, and accounting; integrated safety analysis; safety; etc.) at fuel cycle facilities. An individual asked why an independent accessor would be needed for the cyber security program when one is not needed for the physical security program. The individual also questioned how licensees would be expected to respond if the NRC was not satisfied with the findings of the authorizing official. Multiple industry representatives expressed concern and uncertainty on the need, purpose, and role of the independent assessor and authorizing official.

Session 3 – Identification of Digital Assets within Scope

The NRC described the analysis licensees would need to undertake to identify digital assets that could be compromised through a cyber attack that results in a consequence of concern. Licensees would need to ensure that the analysis extends to the support systems that assure the digital assets function correctly. Once the digital assets are identified, licensees would implement a risk-informed screening methodology to identify alternate controls that would prevent the consequence of concern or implement additional controls, if needed.

One individual asked why safety consequences of concern have a security component. The NRC staff will take another look at the consequences of concern to ensure they are accurate.

An individual stated support systems should only include items identified in the design documentation as being necessary for the digital asset to perform its function. Another individual expressed concern that analyzing support systems has the potential to dramatically increase the scope of the proposed rulemaking. An individual suggested that a laptop used to calibrate a digital asset should not be considered a support system since it is not necessary for the digital asset to perform its function. Rather the laptop may need to be evaluated as an attack pathway, rather than a support system. The individual stated the NRC should draw a distinction between support systems and attack pathways.

Several commenters requested that the NRC provide guidance on how far removed the support system can be from the digital asset to be out of scope. They also asked if the timing required for the consequence of concern to occur would have an impact on the need to protect digital assets. They asked if time could be used as a compensating control. For example, some events occur over long periods of time following the initial cyber attack (e.g., time to drain pool, failure of environmental controller). The NRC should clarify to what extent licensees can credit the ability to detect and intervene in a timely manner.

An individual requested the NRC provide guidance on how to do the analysis to identify digital assets. The NRC is working to develop guidance to accompany the proposed rule language. An individual noted that a system such as a badge reader which protects against unauthorized access should be regulated under the security requirements and not be regulated by cyber security. Also, the loss or disclosure of classified information should be regulated under 10 CFR Part 95 and not under cyber security. The issue of insider threat was also raised. Existing regulations do not require analysis of the insider threat for Category III or 10 CFR Part 40 fuel cycle facilities. Licensees asked if the cyber security rulemaking would require licensees to expand their integrated safety analysis or security programs to address threats previously considered not applicable, e.g., the insider threat. Also, since the insider threat was not considered relevant in the past, including it for cyber security does not appear justified.

There was a discussion on whether the screening criteria would apply to active consequences of concern. The NRC staff indicated that barriers could be used to protect against an active consequence of concern and alternate controls would apply to latent consequences of concern. Industry requested the NRC to provide more clarity on the difference between barriers and alternate controls and to provide an updated flow chart on the screening criteria.

Session 4 – Application of Adequate Controls

The guidance for the proposed rulemaking would list a baseline set of controls that need to be considered for digital assets whose compromise could result in a consequence of concern. Once the cyber security program is established, an independent analysis of the program would need to be conducted. The results of this analysis would be communicated to the authorizing official along with any residual risk due to known vulnerabilities or controls that are under development. The authorizing official would have responsibility to ensure the program provides the minimum level of adequate protection to comply with the proposed regulations.

Several individuals asked if the scope of the rule would only apply to chemicals and nuclear material under NRC jurisdiction. The NRC staff confirmed that this was accurate. Materials regulated under a State license (e.g., source material or chemicals that do not have a nexus to licensed materials) or other Federal agencies (e.g., Occupational Safety and Health Administration) would not be subject to the cyber security regulations, if approved.

Multiple industry representatives indicated that the National Institute of Standards and Technology approach to a cyber security program, including the authorizing official, residual risk, plan of action and milestones, and independent assessor were developed for the Federal government. Some individuals stated that these aspects of the NIST program should not be applied to the nuclear fuel cycle industry. The fuel cycle facilities have established regulatory practices that include management review and approval (similar to the authorizing official), audits (similar to the independent assessment), defense in depth (similar to residual risk management) and corrective action programs (similar to the plan of action and milestones). These individuals recommended the requirements for the cyber security program be made consistent with existing industry programs, rather than require a completely different regulatory structure.

One individual asked if the cyber security proposed rulemaking would allow licensees to make changes to their plans and programs, provided the changes do not degrade effectiveness. The NRC staff expects to include this concept in the proposed rulemaking.

Several individuals provided comments on the control implementation plans (CIP). One individual indicated that the information required for the CIPs may already exist in multiple documents. The requirement to re-document the information in a redundant location should be avoided. The NRC staff agrees the information could be incorporated by reference. One individual stated that compiling information on a digital asset may represent a vulnerability if the information were shared with an independent reviewer or were inadvertently released. Multiple industry representatives expressed concern that an independent audit would be difficult since the staff with the cyber security expertise are part of the cyber security team. Bringing individuals from outside the facility would be challenging to ensure appropriate security and may introduce vulnerabilities.

Multiple industry representatives expressed concern with the concept of residual risk. The independent assessment and communication of residual risk to the authorizing official is significantly different than the regulatory structure that exists at fuel cycle facilities and would require development of duel programs. The industry has established procedures that require cessation of operations if they identify deficiencies in the system (e.g., residual risk that falls short of adequate protection), or they implement compensatory measures with approval of the

appropriate management. The NRC should consider requirements consistent with these existing programs to reduce unnecessary regulatory burden.

One individual asked if the concept of residual risk represented the difference between the minimum controls needed to ensure regulatory compliance and the ideal controls which would exceed regulatory compliance with some defense in depth. Another individual agreed that the residual risk appeared to represent the gap between the regulatory requirement and the ideal controls. A third individual asked if the concept of residual risk was similar to the integrated safety analysis having multiple items relied on for safety which provide defense in depth. The NRC staff indicated the comments were appreciated.

Multiple industry representatives stated that their existing programs could be adapted to apply to cyber security. Licensees already have designated staff to provide management oversight and approval of safety and security programs, do audits, and implement corrective action programs. They recommend the NRC modify the rulemaking concepts to allow licensees to leverage these existing programs which would help reduce the burden of implementing any new cyber security requirements.

At the conclusion of the meeting, the Nuclear Energy Institute requested that the NRC consider providing additional opportunities to discuss the draft prosed rule language and related guidance. The NRC staff indicated that additional meetings would be considered.