DECEMBER 10, 2015, PUBLIC MEETING SUMMARY AND ATTENDEES LIST FOR DISCUSSIONS ON THE TECHNICAL APPROACH FOR THE PROPOSED CYBER SECURITY RULEMAKING FOR FUEL CYCLE FACILITIES

PUBLIC MEETING SUMMARY

On December 10, 2015, the U.S. Nuclear Regulatory Commission (NRC) staff held a public meeting to discuss the revised technical approach for the proposed cyber security rulemaking for fuel cycle facilities. The U.S. Department of Homeland Security (DHS), Industrial Control Systems Cyber Emergency Response Team provided a brief overview of the cyber security services they provide. The remainder of the presentations was provided by the NRC staff regarding the proposed rulemaking activities.

The DHS representatives presented an overview of free services they can provide to assist owners of Critical Infrastructure (CI) in protecting their systems from and responding to cyber-attacks. If requested, DHS can assess a facility's cyber security program, evaluate the capabilities to respond to an attack, and assist in recovery from an attack. They also collect information provided voluntarily on cyber security events/attacks. This information is made available to owners of CI through a distribution list and can be queried from their website at https://ics-cert.us-cert.gov/. The DHS also provides a monthly cyber security training class in Idaho Falls, Idaho. The DHS team's presentation slides are not available for public release.

The NRC staff provided several documents to stakeholders to support the public meeting (Agencywide Documents Access and Management System Accession No. ML15344A296) including: presentation slides, a technical issues document, and samples of draft control sets and related parameters. The NRC staff's presentation consisted of an overview of the National Institute of Standards and Technology (NIST) Risk Management Framework (as described in Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems"), overview of the screening criteria with examples, discussion of the draft Facility-type approach to control sets, and the staff's approach to drafting proposed rule language. Information on these topics is available in the meeting documentation.

Stakeholders raised a number of issues for discussion during the presentation. Some of the significant issues raised include the following items.

Industry representatives expressed agreement with the removal of emergency preparedness for all facility types and material control and accounting for Category III facilities, from the list of systems that require digital assets to be evaluated for consequences of concern. Only digital systems that could impact the safety, security and safeguards systems must be evaluated.

During the overview of the six steps in the risk management framework, a member of the public observed an error on slide 5. The slide should indicate that digital assets must be identified first, then evaluated to determine if there is a potential for an active or latent consequence of concern.

The Nuclear Energy Institute (NEI) indicated that the NRC guidance should establish specific criteria that clearly defines which systems and components need to be protected by cyber security controls. Industry representatives have observed from the power reactors that the

scope of digital systems that need to be evaluated and protected tends to increase over time due to inspections and non-specific guidance.

Stakeholders indicated that the screening examples were helpful, but raised a few additional concerns (e.g., cumulative impact block, timely manner, etc.). Industry representatives encouraged the NRC to develop similar examples on how to implement control sets to required digital assets and creating the System Security Plans (SSPs).

Industry representatives raised concerns that the number of NRC proposed cyber security control sets were too large and not graded. The NRC is seeking to grade the control sets based on the consequences of concern and associated facility type. Two separate control sets and an overlay (additional controls are added to control sets 1 and 2) have been developed that can be applied based on the facility type. An industry representative proposed that the NRC allow licensees to choose which controls are applicable, rather than be required to implement a prescriptive set of controls. Allowing licensees to choose could be similar to the process used during the selection of items relied on for safety (IROFS) in the Integrated Safety Analysis. Under the current proposal, the NRC staff selects the number of controls in a control set based on the consequences of concern and associated facility type. In many cases, the licensee would be able to further reduce the number of controls by documenting the reason that the control is not applicable to specific asset types, establishing common controls, or demonstrating that compensating controls are provided.

A number of industry representatives expressed concern that the documentation needed to maintain over a hundred controls for each digital asset in scope would be excessively burdensome with minimal safety benefit.

There was discussion on the difference between active and latent consequences of concern. Industry requested clarification on whether digital IROFS and sole IROFS would need to be evaluated as active or latent consequences of concern. IROFS are evaluated through the latent analysis. Only events that could be directly induced by a malicious actor would be addressed under the active analysis.

Industry representatives identified a number terms referenced in the technical issues document that are not well defined. They commented that the reference to “high control baseline,” “moderate control baseline,” “insider threat program,” etc. be defined. In several cases, these terms have been adopted from the NIST guidance documents.

The concept of an independent assessment was discussed extensively. Licensees asked if the independent assessment would need to be done by an individual or group outside of the licensee’s organization. They indicated this could be expensive and unnecessarily require them to hire contractors. The NRC staff envisions that licensees could use staff from within their organization, provided the assessment team was selected from a separate entity (independent of the staff involved with identifying and protecting digital assets). Licensees commented that the technical qualifications needed to do the assessment could make it difficult to find qualified staff from within the same organization. In addition, industry representatives commented if the NRC should conduct the independent assessments. NRC staff stated that the details regarding this assessment process were still in the early draft stages and encouraged stakeholders to provide their recommendations.

There were also a number of comments regarding the purpose of the authorizing official. The NRC staff envisions that the authorizing official would be responsible for reviewing the SSPs; the security assessment report prepared by the independent assessment team; and any Plan of Actions and Milestones, in determining whether or not to provide an authority to operate. The licensee, through the authorizing official, would be responsible for documenting the robustness of the controls in their respective SSPs, and the NRC would only inspect proper implementation of the SSPs. Several industry representatives commented that the NRC would need to establish clear documentation for inspectors reviewing implementation of the SSPs to limit the number of discrepancies between the licensee and the NRC.

During the discussion on the revalidation of controls, one commenter proposed the NRC consider a five year revalidation timeframe rather than a three year timeframe for consistency with existing programs (i.e., Process Hazard Analysis).

One industry representative expressed concern that the bulk of the implementation information was going to be placed in the guidance. Since guidance is only one approach that is acceptable to the NRC, licensees may choose alternate approaches, provided the licensee demonstrates compliance with the regulations. The NRC staff is still developing the proposed rule language and is evaluating which concepts can be placed in the rule and which will remain in guidance.

At the conclusion of the meeting, industry representatives identified a number of areas the NRC staff should consider for improvement in the technical approach, such as:

- The NRC should provide examples of the control sets applied to digital assets;
- The wording in the consequences of concern should be further refined;
- The NRC should determine how dual regulation will be addressed between the NRC and other government agencies/contracts (e.g., Naval Reactors), especially for unclassified networks; and,
- The NRC should apply lessons learned from the power reactor cyber security rulemaking.

The NRC staff expressed appreciation for individuals in attendance at the meeting and for individuals who joined the teleconference/webinar. Additional meetings will be scheduled to further discuss the control sets, the proposed rule language and its associated guidance document. The NEI proposed holding the next public meeting on cyber security in March as part of their fuel cycle oversight council. The NRC staff indicated they would consider the proposal, but another meeting in February may also be needed.

Attendees Sheet for Public Meeting on Cyber Security Rulemaking for Fuel Cycle Facilities
December 10, 2015

First Name	Last Name	Organization
Joan	Rolf	NSIR
Gary	Clark	MOX Services
Dealis	Gwyn	MOX Services
Aaron	Kent	MOX Services
Nima	Ashkeboussi	NEI
Janet	Schlueter	NEI
William	Gross	NEI
P. Bennett	Tomlinson	D. Tech. LLC.
Michael	Birchfield	NFS
Brad	Bergemann	NMSS/CSD
Charity	Pantalo	NRC/CSD
Brad	Bergemann	NRC/CSD
Jim	Andersen	NRC/CSD
Casey	Priester	NRC/CSD Contractor
Mike	Shinn	NRC/CSD Contractor
John	Walley	NRC/CSD Contractor
Suzanne	Ani	NRC/NMSS
Matt	Bartlett	NRC/NMSS
Nick	Baker	NRC/NMSS
James	Downs	NRC/NMSS
Brian	Smith	NRC/NMSS
Cardelia	Maupin	NRC/NMSS
James	Maltese	OGC
Jack	Roe	Talisman
Tim	Corcoran	AREVA
Linda	Freepons	AREVA
David	Teyssier	AREVA
Jennifer	Hawley	BWXT
Tony	Martin	BWXT
Brent	Neas	BWXT
Andrew	Rander	BWXT
David	Spangler	BWXT
Joe	Brown	Centrus Energy
Gregory	Corzine	Centrus Energy
Mario	Robles	Centrus Energy
Jana	Bergman	Curtiss-Wright

First Name	Last Name	Organization
Nick	Duan	D. Tech. LLC.
Bennett	Tomlinson	D. Tech. LLC.
Brian	Buckley	GE
Danny	Stewart	GE
Drew	Williams	GE
Tom	Burns	Public
Gary	Hamby	Honeywell
Mark	Wolf	Honeywell
Lidia	Litinski	Honeywell
Shirley	Xu	NRC
Jonathan	Stone	NRP
Edwin	Lyman	UCS USA
Amy	Johnson	Urenco
Bryan	McGowen	Urenco
Joe	Brown	USEC
Alan	Batten	Westinghouse
John	Hentschel	Westinghouse
Nancy	Parr	Westinghouse