November 24, 2015

MEMORANDUM TO: Brian W. Smith, Senior Project Manager
Cyber Security Team
Division of Fuel Cycle Safety, Safeguards,
and Environmental Review
Office of Nuclear Material Safety
and Safeguards

FROM: Matthew Bartlett, Project Manager **/RA/**
Enrichment and Conversion Branch
Division of Fuel Cycle Safety, Safeguards,
and Environmental Review
Office of Nuclear Material Safety
and Safeguards

SUBJECT: OCTOBER 22, 2015, PUBLIC MEETING SUMMARY FOR THE PRESENTATION ON THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBER SECURITY AND DISCUSSIONS ON THE TECHNICAL APPROACH FOR THE PROPOSED CYBER SECURITY RULEMAKING AND RELATED GUIDANCE

On October 22, 2015, the U.S. Nuclear Regulatory Commission (NRC) staff held a public meeting to support the proposed fuel cycle cyber security rulemaking. The NRC staff provided the technical approach under consideration for the proposed rule and proposed guidance based on the cyber security standards developed by the National Institute of Standards and Technology (NIST) (NIST Special Publication 800 series). The meeting was attended by representatives from the fuel cycle industry, the Nuclear Energy Institute, several members of the public, and a NIST representative. The attendance list is provided as Enclosure 1. The slide presentations for this meeting are enclosed (Enclosures 2 and 3).

During the morning session, a representative from NIST provided an overview of managing cybersecurity risk. This presentation covered the cyber security threats, the risk management framework, and information on how to adapt NIST standards to the nuclear fuel cycle industry. The applicable cyber security standards include NIST SPs-800-30, -37, -39, -53, -53A, and -82.

The afternoon session involved a technical discussion on the proposed cyber security rulemaking. The NRC staff provided a document to facilitate the discussion entitled, “Technical Issues for Consideration Regarding the Fuel Cycle Cyber Security Proposed Rulemaking,” available in the Agencywide Documents Access and Management System (ML15288A503).

CONTACT: Matthew Bartlett, NMSS/FCSE
(301) 415-7154

The NRC staff discussed the types of digital assets that would be within the scope of the rulemaking, the grading criteria for determining the level of controls to apply to digital assets, and the screening criteria envisioned for determining when additional controls are needed.

During the technical discussion, participants identified a number of issues, including the following:

1. Clarification was requested on the meaning of the term “compromise of a function.” The term compromise should be clearly defined in writing so that it is not open to interpretation over time.

2. Clarify the extent to which licensees must evaluate support systems (e.g., power supply, communications) that maintain the availability and reliability of safety and security systems under the proposed rulemaking.

3. The proposed technical approach indicates that licensees would need to evaluate digital assets of support systems that could adversely impact safety, security, emergency preparedness and material control and accounting. The NRC staff should clarify the phrase “adversely impact.”

4. The proposed rulemaking should make clear to what extent classified networks would need to be evaluated and to what extent licensees may take credit for compliance with non-NRC regulatory requirements or authorities. The proposed rulemaking should also describe how licensees would avoid dual regulation.

5. The concepts of “active” and “latent” consequences of concern were introduced by the NRC at this meeting. Industry requested if latent consequence could be interpreted as degraded items relied on for safety (IROFS). The NRC indicated that the concept of degraded IROFS would be included in the definition of latent, if the degradation is associated with a consequence of concern.

6. The definition of “consequences of concern” should not reference performance requirements. The phrase is broad and includes a risk component which does not support the idea of establishing a quantitative threshold. The NRC staff agreed that references to performance requirements should be replaced with specific thresholds.

7. Since the proposed guidance will reference the NIST standards, the NRC staff should include in the proposed guidance an option to use equivalent standards such as International Standards Organization 27000.

8. The NRC should consider removing the requirements to evaluate emergency preparedness assets. The NRC staff noted that communications are the primary area of interest and these communications typically have substantial redundancies.

9. The proposed rulemaking should clarify if licensees would be required to conduct a risk assessment and document the findings in a security plan that is submitted to the NRC for approval.

10. The proposed rulemaking or guidance should clarify the role of the Authorizing Official.

11. The NRC staff should clarify if the proposed rulemaking will require licensees to develop and submit for approval a facility Information System Security Plan (ISSP).

12. Examples of the screening criteria should be expanded in future meetings. The NRC staff emphasized that the screening criteria in the proposed guidance would allow licensees to take credit for alternate, equivalent controls (e.g., non-digital IROFS) that could be used in place of implementing additional digital controls.

13. An individual asked what physical security requirements apply to conversion and deconversion facilities licensed under Part 40. The NRC staff noted that the existing requirements are based in part on security orders.

The issues raised by stakeholders, including the items listed above, will be used to inform the NRC staff's development of the proposed rulemaking and guidance. Additional meetings are planned for December 10, 2015, and late January 2016, to conduct further technical discussions.

Enclosures:
1. Attendees List
2. NIST Slide Presentation
3. NRC Slide Presentation

11. The NRC staff should clarify if the proposed rulemaking will require licensees to develop and submit for approval a facility Information System Security Plan (ISSP).

12. Examples of the screening criteria should be expanded in future meetings. The NRC staff emphasized that the screening criteria in the proposed guidance would allow licensees to take credit for alternate, equivalent controls (e.g., non-digital IROFS) that could be used in place of implementing additional digital controls.

13. An individual asked what physical security requirements apply to conversion and deconversion facilities licensed under Part 40. The NRC staff noted that the existing requirements are based in part on security orders.

The issues raised by stakeholders, including the items listed above, will be used to inform the NRC staff's development of the proposed rulemaking and guidance. Additional meetings are planned for December 10, 2015, and late January 2016, to conduct further technical discussions.

Enclosures:
1. Attendees List
2. NIST Slide Presentation
3. NRC Slide Presentation

DISTRIBUTION: FCSE r/f JDowns, NMSS CMaupin, NMSS BBergemann, NSIR SAni, NMSS PStartz, RII JGilliam, RII MNBaker, NMSS JMaltese, OGCNStAmour, OGC CMaupin, MSTR CPantalo, NSIR FCPriester, NRC Contractor

ADAMS Accession No.: ML15308A503 **Package No.: ML15308A506**

OFFICE	FCSE/ECB	FCSE/ECB	FCSE/ECB	FCSE/ECB
NAME	MBartlett	DMiller	BSmith	MBartlett
DATE	11/09/2015	11/13/2015	11/16/2015	11/24/2015

OFFICIAL RECORD COPY

Attendees Sheet for Public Meeting on Cyber Security Rulemaking for Fuel Cycle Facilities
October 22, 2015

First Name	Last Name	Organization
Timothy	Tate	AREVA
David	Teyssier	AREVA
Andrew	Rander	BWXT
Joe	Brown	Centrus Energy
Kelly	Coriell	Centrus Energy
John	Corrado	Centrus Energy
Chris	Harper	Centrus Energy
Jennifer	Hawley	CWX Technologies
Brian	Buckley	GE
Drew	Williams	GE
Danny	Stewart	Global Laser Enrichment
Leoncio	Estevez	Honeywell
Gary	Hamby	Honeywell
Steve	Kostin	Honeywell
Lidia	Litinski	Honeywell
Bryan	Perriello	Honeywell
Mark	Wolf	Honeywell
George	Simonds	Infrashield
Ayan	Islam	Law Student/ UDC Law
Gary	Clark	MOX Services
Dealis	Gwyn	MOX Services
Aaron	Kent	MOX Services
Nima	Ashneboussi	NEI
William	Gross	NEI
Andrew	Sabisch	NFS
Ron	Ross	NIST
Brad	Bergemann	NMSS/CSD
Philipp	Braaten	NRC
Rodney	Fanner	NRC
Jasmine	Gilliam	NRC
Amy	Hardin	NRC
TR	Rowe	NRC
Melana	Singletary	NRC
Charity	Pantalo	NRC/CSD
Suzanne	Ani	NRC/NMSS
Matt	Bartlett	NRC/NMSS
Craig	Erlanger	NRC/NMSS

Enclosure 1

First Name	Last Name	Organization
Brian	Smith	NRC/NMSS
James	Downs	NRC/NMSS
Brad	Bergemann	NRC/CSD
Casey	Priester	NRC CSD (contractor)
Paul	Rades	NRC/OIG
Norman	StAmour	OGC
Tamara	Bloomer	OGC/WCO
Ebaide	Esoimeme	OIG
Steven	Dolley	Platts
Marvin	Lewis	Public
Jack	Roe	Talisman
Edwin	Lyman	Union of Concerned Scientist
Brandon	Maxwell	Urenco USA
Ricardo	Medina	Urenco USA
Kevin E.	Barber	Westinghouse
Alan	Batten	Westinghouse
Nancy	Parr	Westinghouse
Rick	Vislocky	Westinghouse
Doug	Weaver	Westinghouse
Camille	Zozula	Westinghouse
John	Hentschel	Westinghouse
Brian	Holian	NRC/NSIR
James	Andersen	NRC/NSIR
Russell	Felts	NRC/NSIR