U.S. Nuclear Regulatory Commission Public Meeting Summary

Title: Fuel Cycle Cyber Security Proposed Rulemaking Discussion

Meeting Identifier: 20160994

Date of Meeting: Thursday, August 25, 2016

Location: NRC Complex, NRC Three White Flint North, 11601 Landsdown Street, HQ-3WFN1C03, Rockville MD

Type of Meeting: Category 3

Purpose of the Meeting(s): The purpose of the meeting was to obtain early and substantive input from stakeholders on preliminary draft proposed rule language and the associated preliminary draft proposed guidance document. This activity supports NRC's cumulative effects of regulation initiatives.

General Details:

The NRC staff conducted an all-day public meeting/webinar beginning at 9:00 a.m. eastern standard time (EST) until approximately 5:15 p.m. The meeting was very successful for the staff and stakeholders. It provided stakeholder an opportunity to review and comment on the preliminary proposed rule text and the associated preliminary draft proposed guidance document. In fact, many stakeholders indicated that it was the best stakeholder meeting out of the nine public meetings held. The meeting provided staff and stakeholders a mechanism to exchange valuable information that will be used in further development of the draft proposed rule language and associated draft guidance document.

There were at least 48 attendees at the meeting; 20 signed in remotely on the webinar/webcast with some locations having multiple attendees and 28 physically located in the room. The attendees included: industry stakeholders (25), NRC staff (22), and one member of the public. A complete list of the attendees and the organizations represented is attached.

The summary below provides an overview of the meeting discussions. It is not a comprehensive or detailed record of all of the points made during the meeting. Additionally, it does not represent any NRC policy or decisions on the issues presented.

Summary of Presentations:

The U.S. Nuclear Regulatory Commission (NRC) is initiating a rulemaking to establish new cyber security regulations in Part 73 of Title 10 of the *Code of Federal Regulations* (10 CFR), “Physical Protection of Plants and Materials.” The section proposed is 73.56, “Requirements for cyber security at nuclear fuel cycle facilities.” The objective of this rulemaking is to develop and issue new regulatory requirements for nuclear fuel cycle facility (FCF) licensees that will ensure adequate protection of public health and safety and common defense and security. FCF licensees include those licensed under: (1) 10 CFR Part 70 and authorized to possess or use a formula quantity of strategic special nuclear material (SSNM) as defined in 10 CFR 73.2 (Category I facilities); (2) 10 CFR Part 70 and authorized to possess or use special nuclear material (SNM) of moderate strategic significance as defined in 10 CFR 73.2 (Category II facilities); (3) 10 CFR Part 70 and authorized to possess or use SNM of low strategic significance as defined in 10 CFR 73.2 (Category III facilities); and (4) 10 CFR Part 40 and authorized to operate as conversion/deconversion.

The meeting presentation included the following: a status update and schedule discussion, an in-depth discussion on the preliminary draft proposed rule text, and associated preliminary draft guidance document. A copy of the agenda, PowerPoint presentations, and other documents used during the meeting are available at: ADAMS Accession Number: ML16197A083 – Meeting Agenda; ADAMS Accession Number ML16236A199 - August 25, 2016- Slides Presentation on the Draft Regulatory Guide for Fuel Cycle Cyber Security; and ADAMS Accession Number: ML16221A078 - Proposed Rule Language and Related Draft Regulatory Guide to Support the Public Meeting on August 25, 2016.

.

Status Update and Timeline: The NRC staff provided an update on the proposed rulemaking timeline. The points highlighted included completion of the regulatory basis in March 2016. The final regulatory basis for the rulemaking was completed on March 2016 and was publically noticed in the Federal Register (81 FR 21449). As a result of the completion of the regulatory basis, the staff is now in the proposed rule phase of the rulemaking process and the NMSS rulemaking staff has assumed lead of this aspect of the project. In accordance with the Cumulative Effects of Regulation initiatives, staff indicated that they would appreciate any input from industry in the development of the Regulatory Analysis for the rulemaking. The fuel cycle industry indicated that they is willing to provide cost feedback and indicated that the staff should review the cost analysis from the cyber security for reactors rulemaking.

The staff noted the briefing of the Advisory Committee on Reactor Safeguards (ACRS) briefings in the November and December 2016 timeframe and these meetings are normally open to the public but it will be at the ACRS discretion. The proposed rule package is due to the Commission in March 2017. The staff anticipates that the proposed rule package will be published in the *Federal Register* in the June/August 2017 time frame.

Discussion of Preliminary Draft Proposed Rule Language: The NRC staff discussed with stakeholders changes to the revised preliminary draft proposed rule text since the previous published version on May 19, 2016, (i.e., Agencywide Documents Access and Management System no. – ML16131A115). These changes included: 1.Addition: date for current applicants to submit cyber security plan. (2) Deletions: a. recovery no longer a cyber security program performance objective; b. cyber security control families no longer listed; c. support systems no longer need to be identified and addressed unless associated with a vital digital asset. 3. Other changes: a. reordered the consequences of concern from highest to lowest based on the comprehensiveness of the associated cyber security controls; b. added language clarifying that countermeasures to a cyber attack are taken to address cyber security controls; and c. general edits to the rule language for clarity and alignment with draft regulatory guide.

General Comment: Many of the stakeholders indicated that they appreciated the clarifying information that was added to the preliminary proposed rule text.

Consequences of concern, paragraph c: It was indicated that clarification is needed relative to the phrase “to prevent, mitigate, or respond,” and it was indicated that “to prevent” is probably the appropriate language relative to consequences of concern

Cyber security program, paragraph d: Stakeholders indicated that the preliminary draft proposed §§ 73.53 (d)(2) through (d)(6) needs further clarification and should be more performance based. Stakeholders indicated that as written, the draft proposed language would require a large documentation process for vital digital assets. It was suggested that the NRC staff review the language in § 73.54 for comparison. This issue will be discussed further in the context of the draft proposed regulatory guide.

Cyber security plan, paragraph e: Stakeholders indicated that the preliminary draft proposed rule text needs additional clarification. It was also suggested that the proposed paragraphs (e)(1) and (e)(2) be combined into one provision.

Configuration management, paragraph f. Stakeholders indicated that this section needs to be clarified to clearly indicate that documents generated from this provision will be considered a record subject to NRC's review.

Review of the cyber security program, paragraph g: Stakeholders had a number of comments regarding this preliminary draft proposed rule text. It was indicated that the NRC should look at the language in §§ 73.54 (g) and 73.55 (m) to determine what whether this language will be more appropriate. It was also suggested that further clarification may be needed relative to classified versus unclassified systems.

Event reporting and tracking, paragraph h: Some commenters indicated the draft proposed section needs further clarification.

Records, paragraph i: Commenters indicated that additional clarification is needed relative to "retain all supporting technical documentation." They elaborated that the draft proposed text could be overly burdensome for licensees and has the potential for including numerous documents.

Discussion of the Draft Regulatory Guide: NRC staff led the discussion of an early draft of the proposed regulatory guide, and noted that feedback would be greatly appreciated. Staff encouraged stakeholders to suggest examples for inclusion in the document, to identify text that needs clarification, and to note any errors or oversights. NRC staff also noted that the guidance document provides one method of satisfying the proposed rule.

Draft Regulatory Guide (DRG) Chapters:

A. Introduction: This section discusses the purpose and applicability of the proposed rule; applicability; applicable regulations; related guidance; and the purpose of regulatory guide. No comments were received on this section.

B. Discussion: This section discusses the reasons for the rule development; the background on the rule development; the content of each section; the phase implementation in Table B-1; harmonization with international standards; and documents referenced in the guidance. A number of comments were provided on Table B-1 that outlines timeframes for completing specific milestones associated with the proposed rulemaking. These comments included:

1. What is the basis for the phased implementation? Reactors had 8 years to implement their cyber rulemaking requirements, but the fuel cycle facilities implementation timeframe is only one year.

2. Table B-1 indicates full implementation must take place in 12 months. Would the NRC allow licensees to request an alternate schedule in the Cyber Security Plan?

3. The 180 days to develop the Cyber Security Plan appears woefully inadequate.

4. Hiring Cyber Security Team (CST) members may require significant time (up to a year). This would delay development of the cyber security plan until the staff are available to work. Was this considered in the development of the time frames?
5. The 180 day timeframe envisioned in the DRG appears too short and would not allow sufficient time for new staff to obtain appropriate security clearance.

6. For reactors, the timeframes for implementation were tied to a specific event unique to each facility, e.g., refueling. Could the implementation dates for fuel cycle facilities be handled in the same way?

7. The NRC should provide additional time for implementation, up to 3 – 5 years. This would allow 1-2 years for development of the cyber security plan (1 year for analysis) and 3-4 years for implementation.

8. A timeframe for implementation of 2 to 3 years would be more realistic.

C. Staff Regulatory Guidance:

Subsection 1. General Requirements: Provides an overview of each rule concept

9. If licensees choose to use controls that differ (e.g., different parameters) from those provided in the appendix, will they have to provide some technical justification?

10. Why did the NRC add specific parameters (e.g., timelines) to the cyber security controls?

11. Can the NRC share with stakeholders the basis for the parameters that have been implemented in the cyber security controls?

12. The licensees had difficulty comparing the appendices to each other and to the National Institute of Standards and Technology (NIST), standards. Could the NRC consider developing a matrix approach, similar to the low, medium, high, used by NIST to identify which controls apply to each type of vital digital asset (VDA)?

13. How does the current draft regulatory guide incorporate the concept of acceptance of risk?

Subsection 2 - Cyber Security Program Performance Objectives §10 CFR 73.53(b):

14. The text in section 2.1 on page 13 seems to indicate that licensees need to detect an unknown attack pathway. The text in the first two paragraphs do not provide a clear performance objective for detection. Can this text be clarified?

15. Are there detection controls that accomplish the network monitoring that could be used in place of the text currently in section 2.1 of the regulatory guide body?

16. The second paragraph in section 2.1 states that, “Any unusual activity of communications…” The word “any” implies an onerous burden on licensees. The description of detection process in the second paragraph seems to expand what is required for detection beyond the scope of the draft proposed rule language.

17. Licensees use a wide range of assets, some of which are stand alone. Does the NRC plan to require licensees to connect standalone systems to the network in order to monitor their network traffic?

18. The purpose of the regulatory guide is to demonstrate one acceptable approach to comply with the regulations. As such, it should not include optional good practices which inspectors and licensees may misconstrue as items necessary to comply with the regulations.

19. The guidance on detections appears to be a side note that is not necessary to demonstrate compliance with the regulations. The NRC should consider removing the adjectives in the

guidance which makes the guidance open to interpretation and leaves a significant grey area.

20. The fourth paragraph under 2.1 states that, "licensees should review the cyber security detection data and external intelligence information on a quarterly basis…" Does the NRC intend to provide quarterly intelligence briefings for licensees? The guidance should clarify what intelligence data should be reviewed?

21. The NRC should consider the cost required to review external intelligence data quarterly. At a minimum, this cost should be included in the regulatory analysis.

22. Consider stating that licensees need to consider "… relevant …" intelligence sources. The NRC should consider the cost associated with accessing these intelligence sources.

23. The phrase "timely manner" is used multiple times throughout the document (see paragraphs 2, 3, and 5 of section 2.1) but often in different contexts. In some cases it means annually and in other cases it means immediate. Provide clarification on the NRCs meaning for each use of this phrase.

24. On page 15 in the 3rd paragraph of section 2.3, clarify the meaning of incident response "IR."

25. The 3rd paragraph of section 2.3 states that licensees systems "should be tested regularly." The testing of these systems within operations could cause them to fail resulting in a negative impact. Testing may require applying viruses to the systems which may cause them to fail. Consider stating that table tops are an acceptable approach for performing adequate testing, especially in the context of plant operating systems.

Subsection 3 - Cyber Security Team (CST) § 10 CFR 73.53(d)(1):

26. Consider stating that the CST oversees rather than implements the cyber security program.

27. Section 3.2 under "Qualification" indicates the licensee must do "penetration testing." This type of testing could be catastrophic because it could impact operations. The NRC should allow table top exercises to be sufficient.

28. The requirement to test for vulnerabilities needs clarification because the licensees cannot test for new types of attacks before they occur.

29. The requirement to test the industrial control system (ICS) may cause it fail. The guidance on testing could require the licensee to break their own systems.

30. The core of the Industrial Control Systems – Cyber Emergency Response Team of the U.S. Department of Homeland Security (ICS-CERT) is not applicable to a production facility. Many of the exiting plant systems have not previously been tested. The current guidance on testing would require these systems to be tested in place on the operations floor. Their failure may cause a process upset. The NRC guidance should distinguish between operations testing (OT) and information technology (IT).

31. Many of the performance objectives for the CST listed in C.3 are covered in the cyber security controls and should not be included in body of the RG. Including controls in the body makes them appear a necessary commitments needed to comply with the rule language, even though the requirement is not in the rule.

32. The Regulatory Analysis should include costs associated with penetration testing that are discussed in this section.

33. The qualifications listed in section C.3.2 are not consistent with reactor guidance in RG-5.71. What was the NRC's basis for these qualification requirements? Operating reactors have not identified any problems with identifying the appropriate qualification for the CST without guidance.

34. The 12th bullet in requirements for the CST states that licensees need to "Maintain expert skill." Consider removing "expert skill" from the guidance as this term is not well defined.

Subsection 4 - Cyber Security Plan (CSP) § 10 CFR 73.53(e):

35. There is too much specificity on what should be included in the plan. Consider reducing the specificity to only state what is needed to comply with the regulations.

36. The second paragraph of section C.4.1 indicates that "…implementing policies and procedures are protected …" which seems to imply the information must be treated as safeguards. Consider replacing "are protected" with phrase" "are evaluated."

37. The second paragraph of section C.4.1 refers to Part 25 which appears to be a typo. The reference should be Part 95.

38. The regulatory guide should contain some guidance on what documents need to be protected and at what level. The need to protect new documents should be included as a cost in the regulatory analysis.

39. The second to the last bullet on page 19 (section C.4.1) seems redundant.

40. The final 3 paragraphs of sections C.4.1 state that the cyber security plan would be revised and updated as part of the biennial review. The NRC should consider removing the third paragraph in section C.4.1. The NRC should also clarify that the plan only needs to be updated if significant changes have occurred which impact the plan.

41. The last sentence of the final paragraph in section C.4.1 states that the licensee would need to protect the plan. The NRC should consider removing this sentence or the entire paragraph because licensees already know, and have guidance, on how to protect these types of documents.

42. The guidance is unclear on whether licensees should develop an incident response (IR) plan or if the IR would be part of the emergency plan. A requirement to maintain an IR plan separate from the emergency plan may be confusing for the licensee to implement and maintain. If the cyber attack results in a consequence of concern, licensees would use the emergency plan rather than the incident response plan.

43. The guidance on IR seems to imply licensee would need to form a "white-hat team" to do a deep level analysis of the cyber attack. Licensees often do not have the time or resources to conduct this level of analysis for every attack and rely on outside resources.

44. The body of the regulatory guide seems to overlap with many of the controls. Consider referencing the controls, rather than including redundant guidance in the body.

45. The guidance seems to imply that the CST is responsible for IR. Clarify if the IR team must be part of the CST. Consider clarifying that a member of the CST can serve on the IR team or EP team.

46. The first paragraph on page 21 indicates that the IR documentation should be reviewed every 12 months. Consider modifying this timeframe to be consistent with the biennial review.

47. Modify the requirement to update copies of the IR plan to include "as needed" otherwise licensees would need to update their documents, even if there is no change. Also, the guidance should not indicate the documents will be distributed to all staff. Consider replacing "distributed" with "available."

48. Consider deleting the first line on page 21 because it contains too much detail for guidance.

49. Consider deleting the last sentence in the first paragraph on page 21. Licensees already have programs and procedures in place to determine the appropriate protection of documents.

50. Licensees don't have the time and resources to revise and update procedures following every cyber attack. Consider removing the requirement to incorporate lessons learned into formal procedures "following the event" as stated in the fourth paragraph on page 21.

51. Revise the first sentence of paragraph 4 on page 21 to clarify that reaching safe shutdown is the priority over analysis or eradication of malware. Clarify that the analysis and eradication can be conducted after the systems are safe.

52. Since tools are needed to respond to a cyber attack, would they need to be protected as vital digital assets if they could be degraded by a cyber attack?

53. Consider revising the first sentence of paragraph 5 on page 21 to ensure the list of actions following an attack are ordered in level of importance. Consider removing the wording, "manufacturers to be aware of potential vulnerabilities."

54. Clarify the relation between IR and EP. Consider allowing the IR to trigger the EP or vice versa.

55. Consider adding bracketed text to the cyber security plan template in Appendix A to clarify when certain sections can be disregarded by certain licensees.

Subsection 5 - Consequences of Concern § 10 CFR 10 CFR 73.53(c):
General Comments

56. The NRC should not extend cyber security to facilities that do not have some form of a designed basis threat.

57. The NRC should consider limiting digital assets to items that are part of the integrated safety analysis (ISA).

58. The NRC should consider some way to more efficiently get through step 1 of the analysis (identifying digital assets).

Subsection 6 - Identification of Digital Assets § 10 CFR 73.53(d)(3)

59. Consider moving the last 3 bullets of section 6.1 and leading text into the VDA section?

60. Does the Intrusion Detection Systems apply to physical and logical systems?

61. Would material control and accounting (MC&A) move to the VDA section?

62. Do critical target area (CTA) cover the same scope as ISA? Does this rule cover broader scope than CTA?

63. Can licensees take credit for the diversity of multiple digital assets as an alternate means of protection? Can the NRC provide more guidance on how diversity could be used as an alternative means?

64. Can the NRC provide some guidance on how air gapped systems are beneficial? Can the NRC add an appendix on how air gapped systems benefit and how controls apply to these systems?

65. Licensees may use several different operating systems (Windows and Linux) on the same Network. Could the licensees credit these as alternate means and if so, under what conditions?

66. NRC should consider using language on alternate means from page 8 of AO1310, which was used for 10 CFR 73:54.

67. Provide some clarification on what NRC means by air gapped (e.g., non-internet facing, data diode, etc.)

68. What does the phrase, “The consequences of concern, ranked in order of highest to lowest…” mean? Does this ranking have any relationship to the ranking of item(s) relied on for safety (IROFS) in the ISA?

69. The verbal description of ranking provided by the NRC at the meeting is clearer than the exiting explanation in the guidance. Consider revising the guidance to improve the explanation.

70. The bullets describing the support systems in section C.6.3.2 provide a better explanation than other text on support systems throughout the document. Can similar text be used in place of the existing explanation located in the other sections of the guidance?

71. The guidance on the boundaries for vital digital assets in section 6.3.1 is confusing. Is this consistent with the systems approach (not clear)?

72. Can the NRC include some scenarios as examples of support systems and boundaries for VDAs?

73. If you have an application that fits into your MC&A database, would your entire network need to be scoped in? Since applying controls at the network level and since the network is needed, under 6.1 wouldn’t controls have to apply to the whole network since it is supporting the VDAs?

74. If a widget is VDA, according to bullets in this section, the network is feeding a VDA. Would the network be considered a VDA?

75. If someone injects malicious input into VDA on MC&A and a network is needed to input code, would the network be scoped in as a support system of VDA? If so, networks may need to be separated into sections. Additional information is needed on what a VDA is. It appears that the entire network would require protection.

76. Can licensees take credit for existing insider mitigation personnel programs to eliminate the need to consider malicious actor events?

77. Do licensees need to consider pathway that malicious software travels through to reach the VDA as a VDA since it supports the VDA?

78. Is the support system used to reach a VDA considered a VDA?

79. In MC&A, if endpoints reach out to the applications and you lose accountability due to malware, then this is consequence of concern (COC). Therefore, wouldn't the network be a support system whose compromise could result in a consequence of concern?

Subsection 7 - Cyber Security Controls §§ 10 CFR 73.53(d)(2) and (d)(5)

80. Good work reducing number of controls. However, still some areas where controls do not directly apply to COC. These controls could be removed along with those controls that focused on good operational practices.

81. In Section C.7.3, concern with the language about unannounced tests, malicious actor testing, and mode testing. Also, who are the assessors? Are the assessors members of the CST?

82. The performance and load testing are not an IT cyber security attack item but is more IT operations. Also, unannounced tests to the IT department are not what we want to be doing to someone else's hardware.

83. Will NRC change the text on page 31 paragraph 3 which prohibits a single countermeasure from satisfying multiple controls?

84. The NRC is encouraged to provide additional guidance on unplanned assessment and vulnerability assessments. The NRC should consider using NIST PL-6 (Security-Related Activity Planning, Security and Privacy Controls for Federal Information Systems and Organizations) controls for vulnerability/scanning. These topics need additional guidance on NRC expectations.

85. Does continuous monitoring of VDA mean 24/7? What does NRC mean by continuous monitoring and how is it applied to different shifts and different types of facilities. Clarify if the NRC means continuous and 24/7 in the main body and the appendices.

Subsection 8 - Implementing Procedures (IP) and Interim Compensatory Measures (ICM) §§ 10 CFR 73.53(d)(5)(ii) and (d)(6):

86. Why is section C.8.4 of the DRG needed? Can this section of the document be deleted? The level of detail and documentation does not add value.

87. Implementing procedures are in 5.ii and compensatory measures in section 6 of the rule, yet they are addressed in one section of the DRG. This is a bit confusing. The text in section 8, with the exception of 8.8, describes type of documentation needed for implementation rather than guidance on how to implement the program using processes and procedures. Some

text should go into identifying VDA sections. Consider deleting all of section C.8 except for C.8.8.

88. Much of the information in C.8.8 are lists of information that could be housed in the analysis. The implementing procedures should tell how to test, audit, and calibrate.

89. If a procedure is already in place to deal with upset conditions, could licensees simply add cyber security to the existing procedures?

Subsection 9 - Configuration Management § 10 CFR 73.53(f):

90. In C.9.2 says VDA can't operate until it is validated. This would seem to imply that the facility needs to be shut down once the rule in approved.

Subsection 10 - Biennial Review § 10 CFR 73.53(g):

91. The requirement to make the biennial review auditable and inspectable is unclear. Does the biennial review include the audits and inspections? What is the relationship between auditable and inspection and the biennial review. Does this mean "inspection are conduced annually"?

92. Good job defining biennial review. Explain bullet 5 on page 39. What is the intent of bullet 5 that says "the license must review the effectiveness of controls?" How does this review differ from the biennial review? Was the use of the phrase "any VDA" intentional? What does the word "any" mean?

93. What is the reference to 70.32(f)?

94. Is there any requirement to file a change plan to the NRC for prior approval?

95. Does this bullet mean that licensees must begin the biennial review one year after implementation of the cyber security program or 2 years?

96. Could this first bullet on page 40 be deleted?

Subsection 11 - Event Reporting and Tracking § 10 CFR 73.53(h):

97. Would NRC consider degradation of a cyber security control a reportable event? These degradations are common but almost never result in an increased vulnerability. Would the process be part of the change control process? Make it clear that items are reportable when they decrease the effectiveness of the control.

Subsection 12 - Recordkeeping § 10 CFR 73.53(i):

98. The requirement to record the list in the DRG is long and the value is unclear. Many of the documents required would not provide value over time. All of these documents would be a lot of data. Keeping all the data can degrade the effectiveness of subscriber identification module because decreases search capability.

99. The ability to retain sufficient information to stand back up what happened would be difficult to maintain. NRC should identify what the goal of retaining the records are to better refine what is required to be saved. The NRC may want to consider maintaining records for 3 years instead of lifetime of plant.

100. Even maintaining the level of records stated in the DRG would be a major effort due to the significant amount of data.

Appendix A: Cyber Security Plan

101. Can the sentences be revised to replace the square brackets to remove the need for the licensee to include their full name? This will make the text less messy since their real name is very long and the name is not needed. Please reconsider the use of any adverb, adjective, or categorical term in the licensing document.

102. Appendix A, page A-1, 4th paragraph, 1st sentence, line 3: It contains the statement "maintain cyber security controls on vital digital assets…" Consider changing "on" to "for."

103. Appendix A, page A-1, 4th paragraph, 2nd sentence, line 4: There is a typo in this sentence. It should be changed to read, "...shall develop compensatory measures, in the event…" Also, the template means that compensatory measures would not be in the plan, they would only be committing to develop the compensatory measures. Since compensatory measures are case specific, detailing them out in a procedure is not good use of resources. Does NRC expect these to be written out in detail ahead of time? Consider modifying the 4th paragraph to state that, "licensees shall maintain the ability to implement compensatory measures in the vent a cyber security control fails as needed." This means licensees will be able to develop and implement in a timely manner.

104. Appendix A, page A-2, Section A-2, Cyber Security Program Performance Objectives, 1st paragraph: The paragraph indicates that the "Cyber Security Incident Response team (CSIRT) is trained at least every 12 months." Two years is more common. Why is 12 months needed? The scope of the timing should be made much narrower.

105. Appendix A, page A-3, Section A-4, Cyber Security Program: Penetration testing is not included in A-4 which is closer to what a cyber security program would look like. A-4 is what an operating cyber security program would look like.

106. Appendix A, page A-4, Section A-4, Cyber Security Program, 1st paragraph: Would including the list of cyber security controls in the cyber security plan, as specified by this paragraph make the plan be controlled as a security related document?

107. Appendix A, page A-7, Section A-7, Biennial Review of the Cyber Security Program, 3rd bullet: This section gives the impression that the biennial review is a whole sale review of all digital assets. This section should be revised.

108. Appendix A, page A-7, Section A-7, Biennial Review of the Cyber Security Program, contains 3 bullets. The 3rd bullet should be deleted.

109. Appendix A, page A-7, Sections A-7, Biennial Review of the Cyber Security Program, and A-8, Event Reporting and Tracking: What is the purpose of having licensees specify the name of their corrective action program? If licensee is required to have a corrective action program, licensee can reference it. But some facilities are not required to have a corrective action program.

110. Appendix A, page A-7, Section A-9, Records: This section indicates a 3 year retention for records, which is better than maintaining documents for the life of the facility, as indicated in the proposed rule text.

111. Appendix A, General Comment: Appreciate reference to cyber security controls, but some power reactors did not want to reference controls without a version number. Or they preferred to include cyber security controls into the regulatory guide. How do you ensure the controls remain updated and do not need to be modified over time without significant impact on the license?

112. Appendix A, General Comment: The NRC needs to allow licensees' programs to remain agile to address the evolving cyber security threat. NRC needs to allow controls to be updated based on the evolving threat.

Appendix B: Controls for VDAs associated with all consequences of concern

113. Appendix B, General Comment: The NRC needs to allow licensees' programs to remain agile to address the evolving cyber security threat. NRC needs to allow controls to be updated based on the evolving threat.

114. Appendix B, General Comment: Keeping consistent with National Institute of Standards and Technology (NIST), Special Publication (SP) 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations, will make it easier for some licensees to implement the controls. If controls need enhancement, call that out in an appendix rather than reinventing all the controls. Consider endorsing NIST controls with exception.

115. Appendix B, General Comment: DOE use to have their own control appendix. They have obsoleted those and gone to a NIST based set of controls with some enhancements. Will be NRC consider doing this as well?

116. Appendix B, General Comment: See cross walks between NIST SP 800-53, Rev. 4 and other standards. If there is much tailoring, the crosswalks become more difficult to use.

117. Appendix B, General Comment: Many of the controls do not have a close nexus to the consequence of concern. NRC should consider limiting the controls tho those that are needed to prevent the COC.

118. Appendix B, page B-1, Section B-1, Detection, bullet 2, Takes the following actions to detect potential cyber attacks, sub-bullet 7, "Update vulnerability information regarding VDAs at least every 7 days:" These controls refer back to NIST SP 800-53, Rev. 4. Those controls are determined by the licensee. If the licensee's cyber security system is built on the NIST standards, would a licensee still need to use the NRC DRG appendices rather than the freedom provided by NIST standards? Could licensees use their own parameters if they provided an independent basis? NRC should allow licensee to use other standards as a basis for applying controls and parameters.

119. Appendix B, page B-1, Section B-1, Detection: If licensee uses other standards, would the NRC issue requests for additional information when reviewing the licensee's cyber security plan? Can stakeholders see the technical basis for each control parameter? Are the parameters tailored based on the types of facilities?

120. Appendix B, page B-2, Section B-3, Separation of Duties: This section would force a level of separation that would be expensive for facilities to implement. The level of separation is beyond what Cat 3 facilities could implement.

121. Appendix B, page B-2, Section B-5, Authorize Access to Security Functions: If a programmable logic controller is on a wall in the plant, everyone has access to it. If an employee's badge allows access, is that okay?

122. Appendix B, page B-4, Section B-18, Continuous Monitoring: For this section, how does NRC envision implementing the last bullet (i.e., "Documenting the security status of the VDAs and their operating environment by the Cyber Security Team (CST) at least every 30 days"). Is this an in depth review or high level review required? Could the wording be changed to remove the phrase "security status"?

Appendix C – F: Additional controls for VDAs based on consequence of concern:

- Contain additional controls that, in combination with the controls from Appendix B, NRC considers adequate to effectively address cyber security for VDAs associated with a particular consequence of concern
- The licensee can choose to adopt these appendices (as applicable) and attach them to their cyber security plan
- If the licensee choose to develop their own controls, it must demonstrate that the controls provide the capability to detect, protect against, and respond to a cyber attack capable of causing a consequence of concern

Next Public Meeting(s): The next public meetings will be held during the formal public comment period(s) for the proposed rule and the draft regulatory guide during the formal which will be noticed in the Federal Register.

Attachments:

1. Meeting agenda – ADAMS Accession No.: ML16197A083
2. NRC staff presentation – ADAMS Accession No. ML16236A199
3. Preliminary Draft Proposed Rule Language and Related Draft Regulatory Guide - ADAMS Accession No: ML16221A078
4. List of Attendees – Attached

August 25 Public Meeting - List of Attendees:

	Last Name	First Name	Organization
1	Anderson	James	NRC/NSIR
2	Ani	Suzanne	NRC/NMSS
3	Antonescu	Christina	NRC/ACRS
4	Ashkeboussi	Nima	Nuclear Energy Institute
5	Baker	Nick	NRC/NMSS
6	Barilla	Frank	Areva
7	Bartlett	Matthew	NRC/NMSS
8	Bergemann	Brad	NRC/NSIR
9	Bergman	Jana	Curtiss-Wright Nuclear
10	Birchfield	Michael	NFS
11	Clark	Gary	MOX Services
12	Corcoran	Tim	Areva
13	Deucher	Joe	NRC/NMSS
14	Downs	James	NRC/NMSS
15	Edwards	Kim	NRC/NSIR
16	Gilliam	Jasmine	NRC/Region II
17	Gomez	Antonio	NRC/NRR
18	Gross	William	Nuclear Energy Institute
19	Gwyn	Dealis	MOX Services
20	Hamby	Gary	Honeywell
21	Harper	Chris	Centrus Energy
22	Hollern	Jason	Areva
23	Jelke	Brian	Sargent Lundy
24	Johns	William	NRC/NSIR
25	Kent	Aaron	MOX Services
26	Lewis	Marvin	Public
27	Liebenon	Michael	Areva
28	Link	Robert	Nuclear Energy Institute
29	Litinski	Lidia	Honeywell
30	Maltese	Jim	NRC/OGC
31	Maupin	Cardelia	NRC/NMSS
32	Moore	Johari	NRC/OC
33	Neas	Brent	General Electric
34	Pantalo	Charity	NRC/NSIR
35	Priester	Andrew	NRC/NSIR (contractor)
36	Richardson	Greg	EPM, Inc.
37	Robertson	Robert	Honeywell
38	Shinn	Michael	NRC/NSIR
39	St Amour	Norm	NRC/OGC
40	Startz	Paul	NRC/RII
41	Stewart	Danny	General Electric
42	Teyssier	David	AREVA
43	Theuret	Robert	Westinghouse
44	Truchon	Brian	Honeywell
45	Trussell	Greg	NRC/NMSS
46	Walley	John	Shine Medical
47	Wijetunga	Suneth	NRC/NSIR
48	Williams	Drew	NRC/NSIR
49	Rogers	Jamie	Nuclear Fuel Services