

PUBLIC MEETING SUMMARY FOR DISCUSSIONS ON CONCEPTS FOR THE PROPOSED
CYBER SECURITY RULEMAKING FOR FUEL CYCLE FACILITIES
FEBRUARY 18, 2016

PUBLIC MEETING SUMMARY

On February 18, 2016, the U.S. Nuclear Regulatory Commission (NRC) staff held a public meeting call to discuss concepts for the proposed cyber security rulemaking for fuel cycle facilities. The presentation included an update of the timeline for the proposed rulemaking, discussion of the nine sections envisioned for the proposed rule, and then topics to discuss at the next public meeting. The summary below represent an overview of the discussions held during the meeting and does not necessarily represent the NRC's final policy on the issues.

The timeline indicates the draft regulatory basis is scheduled to be published in March 2016. The next public meeting is scheduled for March 17, 2016, and will take place in Atlanta, GA. The proposed rule package is scheduled to be provided to the Commission by June 2016. If the Commission approves the SECY paper, the proposed rule package should be published in the *Federal Register* with an opportunity to comment in the December 2016 or January 2017 timeframe.

The stakeholders provided feedback on the NRC staff's concepts for the proposed rulemaking. The discussion touched on whether analog assets should be considered in the cyber security assessment. Industry expressed concern that this would represent a significant expansion of scope, beyond the digital assets that have been discussed in previous meetings. The NRC staff indicated the issues is being considered internally, but resolution is not expected to significantly expand the scope of the proposed rulemaking.

The question was raised on whether the proposed cyber security rulemaking would take into consideration other rulemakings. The NRC staff is maintaining awareness of how ongoing rulemakings may impact cyber security, but the final language would be based on existing regulations at the time of publication.

A member of the public asked to what extent digital IROFS would need to be protected under the rule. Digital IROFS used for safety, security, and safeguards would need to be analyzed as part of the cyber security program, but the need for additional controls may screen out provided other IROFS or systems remained available and reliable to provide equivalent function. Another member of the public questioned if the consequence of concern for radiological and chemical exposures should be set to the same level as the high or intermediate consequences used in Title 10 of the *Code of Federal Regulations* Part 70.61, rather than a combination of the two thresholds.

Several suggestions were proposed by the stakeholders for topics to discuss at the next public meeting in Mach 2016 including:

- discuss the control sets in more detail;
- explain how to determine which controls must be applied and when the controls screen out;
- clarify what constitutes support systems that need additional protection;

- provide more information on how to identify which assets are subject to the proposed rule;
- review the lessons learned from the reactor cyber security rulemaking and Part 73.54; and
- consider discussing the revisions to the regulatory basis and comment resolution document, if it is available.

The NRC staff indicated these topics would be considered for discussion at the next public meeting.

The Nuclear Energy Institute asked if the NRC anticipates publishing any additional documentation prior to the March 2016 meeting. The NRC staff does not plan to publish draft rule language or guidance until the proposed rule comment period. Slides for the meeting may be provided in advance, time permitting.

There was significant discussion regarding independent assessment, reauthorization, and the purpose of the authorizing official. Industry questioned what level of independence would be needed for the assessments. The NRC staff envisions that individuals from inside the facility could conduct the assessment, provide they were not directly connected to the cyber security program. Industry proposed a longer timeframe for conducting the assessment, such as 2 years, in place of the annual timeframe. The current proposal would require all assets to be reviewed annually and the entire program to be reviewed every 3 years. An individual noted that 2 years is the timeframe required for power reactors in 73.54. An industry representative stated that an event due to a cyber attack at a fuel cycle facility is less significant than events that could occur at a power reactor. A member of the public disagreed and stated that fuel cycle facilities have equivalent or even higher consequences of concern. One individual recommended that the cyber security plan should be maintained as a living document and not require excessive regulatory burden to maintain. A person asked if the NRC would need to be the authorizing official. The NRC envisions the authorizing official would be a senior member of the licensee's management.

The NRC staff expressed appreciation for individuals in attendance at the meeting and for individuals who joined the teleconference and webinar. A more in depth discussion of the concepts and guidance for the draft proposed rule language will be discussed at the all-day, March 17, 2016, public meeting.