NOTATION VOTE

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: Commissioner Baran

SUBJECT: SECY-14-0147: Cyber Security for Fuel Cycle Facilities

Approved X Disapproved _____ Abstain _____

Not Participating _____

COMMENTS: Below _____ Attached X None _____

SIGNATURE

2/9/15

DATE

Entered on "STARS" Yes ✓ No ___

Commissioner Baran's Comments on SECY-14-0147
"Cyber Security for Fuel Cycle Facilities"

Introduction

In the paper before us, the NRC staff seeks Commission direction on the appropriate way to strengthen cyber security at fuel cycle facilities regulated by NRC. This paper follows years of discussions with industry aimed at reaching agreement on a meaningful, voluntary cyber security program. Following the terrorist attacks of September 11, 2001, the Commission issued orders to fuel cycle licensees to address certain security measures, but these orders made only a passing reference to cyber security and did not include specific, enforceable cyber security requirements. In 2012, the NRC staff provided the Commission with a Cyber Security Roadmap. The Roadmap reflected the staff's support for a graded approach to developing cyber security requirements commensurate with the safety and security risks associated with each type of facility. For fuel cycle facilities, it noted:

> In the short-term, the NRC is working with NEI and fuel cycle licensees on a voluntary initiative that would strengthen licensee cyber security programs. However, if industry decides not to participate in this voluntary initiative, or if the resulting changes do not generate the desired outcome of strengthening existing fuel cycle facility cyber security programs, Orders will be considered.

We are now at that point.

NRC Staff Efforts to Date

In 2011, the NRC staff established a cyber security working group to review cyber security programs at fuel cycle facilities and to assess whether NRC should require licensees to take additional actions to strengthen cyber security at these facilities. As part of this process, the working group had numerous interactions with licensees and industry representatives. The working group confirmed that fuel cycle facilities are increasingly reliant on digital technologies and that protecting those digital systems from cyber-attacks is crucial.

The working group also conducted site visits to assess the cyber security capabilities of NRC-regulated fuel cycle facilities. What the working group found is sobering. [

]

In an effort to address these vulnerabilities, the NRC staff worked with industry for over two years in the hope of developing consensus on an effective voluntary initiative. The staff sought industry implementation of six measures that would establish a basic cyber security program and security controls:

1) Establish a cyber security team;
2) Provide cyber security awareness training to staff;
3) Establish a cyber security incident response capability;
4) Provide security controls that address portable media, devices, and equipment;
5) Perform a baseline assessment of digital assets performing safety, security, emergency preparedness, and material control and accounting functions to understand the connections between digital assets and other systems, interactions between digital assets, and interdependencies between digital assets; and
6) Provide security controls to isolate digital assets performing critical SSEPMCA functions from external, network-based attack vectors.

These six measures were prioritized from a set of over 200 measures described in the NIST Cybersecurity Framework issued in February 2014. This NIST framework was developed by a public process, through collaboration between government and the private sector, and uses a common language to address and manage cyber security risk in a cost-effective way based on business needs.

Despite the staff's outreach efforts, the fuel cycle facility licensees only agreed to implement the first four NRC-recommended actions. The licensees did not agree to voluntarily implement the two measures that are arguably the most important: identifying key digital assets and vulnerabilities and taking steps to protect those assets from external cyber-attacks. The licensees also did not agree to make any of the modest voluntary measures they were willing to undertake enforceable by including them in their site security plans. According to the staff paper, the licensees' proposed voluntary actions "only consider cyber security threats that result in events causing a potential high consequence outside of the controlled area." That approach fails to address the risks of on-site nuclear criticality, exposure of workers to potentially life-threatening chemical and radiological impacts, and compromised safety and security programs.

Next Steps

The staff has concluded that "additional cyber security requirements are needed to adequately protect the public health and safety and the common defense and security from potential consequences of a cyber-attack." The staff has warned that, if compromised by a cyber-attack, the availability and reliability of SSEPMCA functions required by NRC regulations "could be adversely impacted in a manner undetectable until the function fails to respond when called to perform." According to the staff, these vital functions "are not currently protected in a manner sufficient to adequately protect public health and safety and the common defense and security, and will not have sufficient protection in the near-term with only the implementation of voluntary actions proposed by" the industry and licensees. Based on these conclusions, the staff recommends that the Commission authorize the issuance of a security order to fuel cycle facility licensees requiring basic cyber security measures and a subsequent rulemaking to establish long-term cyber security protections.

I approve the staff-recommended Option 1. In my view, the current cyber security vulnerabilities present at fuel cycle facilities and the lack of agreement by licensees to voluntarily implement an adequate cyber security program to protect against those vulnerabilities necessitates the issuance of an order. A subsequent rulemaking also is needed, but waiting several years for a rulemaking to be completed and implemented would leave fuel cycle facilities vulnerable for too long.

The draft order is well-tailored to address cyber risks in the short term while the rulemaking proceeds. The draft order would establish basic cyber security requirements, focusing on key digital assets. It would require the six actions described above in addition to cyber security configuration management controls and cyber security event reporting requirements. The draft order provides for graded protection utilizing performance-based standards applicable to every fuel cycle facility, so the uniqueness of each facility should not be an obstacle to implementing the draft order. The staff has already prepared guidance to assist licensees with implementation of the draft order.

Regardless of whether an order is issued, I agree with Commissioners Svinicki and Ostendorff that the rulemaking should be a high priority that is completed and implemented expeditiously. We should not allow several more years to pass before adequate protections are put in place. In addition to recognizing the rulemaking as a high priority, I support directing staff (1) to establish a dedicated team to focus on this rule, and (2) to rely on the work done to date to prepare a proposed rule rather than developing a separate regulatory basis document. Through the course of preparing this paper and examining these issues over the past several years, the staff already has completed a significant amount of work (including the working group final report, site visit reports, and summaries of conference calls with licensees) that should enable them to expedite the rulemaking process. Given this existing foundation of technical information, I believe that a separate regulatory basis document is unnecessary.