COMWCO-10-0001

September 14, 2010

MEMORANDUM TO: Chairman Jaczko
Commissioner Svinicki
Commissioner Apostolakis
Commissioner Magwood

FROM: Commissioner Ostendorff **/RA/**

SUBJECT: REGULATION OF CYBER SECURITY AT NUCLEAR POWER PLANTS

SUMMARY

The purpose of this COM is to facilitate a policy decision by the Commission related to the NRC's, the Federal Energy Regulatory Commission's (FERC), and the North American Electric Reliability Corporation's (NERC) responsibilities for cyber security regulation, enforcement, and inspection. The Commission has received staff input and legal analysis to render a policy decision, yet there is no decision-making vehicle currently before us. Recent interactions between the NRC, FERC, NERC, and NRC licensees highlight the desirability of timely action by the Commission on this specific cyber security issue. In summary, and for the reasons explained below, I believe that the Commission should make a policy decision to expand the scope of the cyber security rule (10 CFR § 73.54) such that structures, systems, and components (SSCs) in the Balance of Plant (BOP) at NRC-licensed Nuclear Power Plants (NPPs) should be included within the scope of the rule. Further, the Commission should direct the staff to provide the Commission with an information paper discussing its implementation of this decision, and take appropriate steps to inform NRC licensees, NERC, and FERC of the Commission's decision.

BACKGROUND

In January 2008, FERC issued Order No. 706, which specified Critical Infrastructure Protection (CIP) Reliability Standards to safeguard critical cyber assets. The requirements in Order No. 706 apply to certain users, owners, and operators of the bulk-power system, but specifically exempt "facilities regulated by the NRC." In March 2009, the Commission issued a final rule, 10 C.F.R. § 73.54, which set forth cyber security requirements applicable to NPP licensees.

This regulation was intended to apply to digital SSCs within an NPP that, if compromised, could result in radiological sabotage.

As a result of interaction with the NRC staff after issuance of Order 706, in March 2009, FERC issued Order No. 706-B to ensure that no regulatory "gap" existed between the NRC's and FERC's cyber security requirements as they apply to NPPs. Specifically, Order No. 706-B clarified that the BOP equipment within an NPP that is not covered by the NRC's cyber security regulation is subject to compliance with the CIP standards approved in Order No. 706. However, Order 706-B also established a process through which NPP licensees could apply for an exception to the CIP standards "to the extent that the licensee believes that specific equipment within the balance of plant is subject to NRC cyber security regulations." NERC is the FERC-certified electric reliability organization responsible for inspecting digital assets related to reliability of electrical power at NRC-licensed NPPs. The NRC and NERC committed to cooperate in considering specific exception requests from NPPs in a December 2009 memorandum of understanding (MOU) discussed further below.

In October 2009, the NRC staff briefed the Commission on, *inter alia*, NRC and NERC cyber security jurisdictional issues, cyber security inspections at NRC-licensed NPPs, and the status of the MOU between the NRC and NERC. [redacted]

In December 2009, the NRC and NERC signed an MOU that sets forth and coordinates the roles and responsibilities of each organization as they relate to the application of respective cyber security requirements at NRC-licensed NPPs. Although this MOU generally describes the jurisdictional delineation of cyber security authority over NPP SSCs between the NRC and NERC, it does not specifically identify SSCs that are subject to either NRC or FERC jurisdiction.

In May 2010, NERC issued a "bright-line" survey to NRC NPP licensees to determine which NPP SSCs should be exempted from FERC cyber security jurisdiction. The "bright-line" survey provided two generic lists of BOP SSCs – one list of SSCs potentially subject to FERC CIP standards, and one list of SSCs potentially subject to NRC cyber security regulations. All NRC

NPP licensees declared in their survey responses that the BOP SSCs identified as potentially subject to the FERC CIP standards are, in fact, within the NRC's cyber security regulations because those BOP SSCs are "important to safety." NERC is required to report the results of the "bright-line" survey to FERC by October 15, 2010.

In a letter dated August 9, 2010, NERC informed the NRC that based on the "bright-line" survey responses, NERC has determined that the assignment of regulatory authority for the BOP SSCs from the NERC CIP standards to the NRC cyber security authority is conditionally acceptable. To date, however, the Commission has not made a determination on this important policy matter.

On August 27, 2010, NERC sent letters to NRC NPP licensees requiring that they provide a notification letter to the NRC that identifies all BOP SSCs considered important to safety, and requiring that they submit a revised cyber security plan to the NRC for review and approval.

DISCUSSION

From discussions with my Commission colleagues, the NRC staff, and external stakeholders, it is clear to me that there is a common objective and associated advantages of having the NRC as the single Federal entity regulating and inspecting cyber security onsite at NRC-licensed NPPs. It is more efficient for the Federal government to apply one set of cyber security standards onsite at NPPs, and to have the NRC inspect against those standards. The NRC has qualified inspectors who are routinely on-site, very knowledgeable of nuclear power plant SSCs, and highly competent to perform effective cyber security inspections. In addition, it is my understanding from discussions with the NRC staff that FERC and NERC's main interest in such an arrangement is whether the NRC's cyber security requirements are at least as robust as FERC's, and that, in fact, the NRC's cyber security requirements are more robust than FERC's.

The absence of a Commission policy decision in this matter makes it very difficult for the Federal government and NRC NPP licensees to move forward in a timely manner to establish an effective and efficient arrangement for the Federal regulation and oversight of cyber security at NRC-licensed NPPs. This challenge is noted in the related correspondence from NERC in August 2010.

For instance, in its letter to the NRC dated August 9, 2010, NERC stated the following:

> In order for NERC to satisfactorily fulfill its obligations under the FERC Order No. 706-B requirements to ensure that there is no gap in regulatory coverage, and after the NRC receives the notifications from the NPPs, NERC requests the following:

1. An affirmation from the NRC to NERC, that the NRC has accepted the NPP's letter of commitment declaring that all of the balance of plant SSCs are "important to safety" and within scope of the requirements of 10 C.F.R. §73.54; or

2. A letter from the NRC to NERC, declaring that the NRC does not accept the NPP's letter of commitment stating that the balance of plant SSC's are important to safety and therefore within the scope of 10 C.F.R. §73.54.

Further, in its letter to NRC NPP licensees dated August 27, 2010, NERC stated the following:

> In order for NERC to verify that these BOP SSCs are covered under the NRC's jurisdiction, and therefore not subject to NERC jurisdiction, NERC is requiring that each NPP provide the NRC with a notification letter identifying all BOP SSCs considered important to safety. Additionally, NERC is requiring that each NPP submit a revised cyber security plan to the NRC for its review and approval. If the NRC determines that these BOP SSCs are not within the scope of its jurisdiction, these BOP SSCs will remain subject to compliance with the applicable NERC CIP Reliability Standards as identified in the FERC-approved NPP implementation plan. At such time, NERC may initiate an on-site Spot Check audit within 30 calendar days in accordance with the NERC Compliance Monitoring and Enforcement Program ("CMEP").
>
> NERC is requiring each NPP to submit the notification letter described above to the NRC, with a copy to NERC within thirty (30) calendar days after receipt of this letter.

The above excerpts from NERC's correspondence highlight an important policy question for the Commission: specifically, should the BOP SSCs at NRC-licensed NPPs be considered "important to safety" for the purpose of being considered within the scope of 10 C.F.R. § 73.54?

In my view, the answer to this question should be "yes." I have carefully reviewed the record of Commission decisions and OGC's March 8 memorandum on cyber security. I recognize that the NRC's cyber security requirements in 10 C.F.R. Part 73 have been interpreted to cover only those SSCs that could directly or indirectly result in radiological sabotage. Nevertheless, I believe that the cyber security of NRC-licensed NPPs is an issue that has a nexus to the protection of public health and safety from the hazards of radiation, is a matter of great national importance, and involves a unique set of circumstances. The Commission has enough

information before it to make a policy decision on this matter. Therefore, I propose that the Commission use its broad authority under the Atomic Energy Act to generically determine that SSCs in the BOP at NRC-licensed NPPs are "important to safety" for purposes of being within the scope of 10 C.F.R. § 73.54. Interpreting the rule in this matter would result in regulation, inspection, and enforcement of cyber security requirements at NPPs by a single Federal regulator -- the NRC.

The Commission's resolution of this policy question will help the Federal government provide clarity and stability in its regulatory framework for the oversight of cyber security at NPPs. Furthermore, resolution of this matter will help to minimize dual regulation concerns and enable more efficient use of Federal government resources. I believe that timely resolution of this matter is of great importance to the NRC, FERC, NERC, and the regulated community.

To give effect to this decision, I propose that the staff be directed to provide the Commission with an information paper by October 30, 2010, that outlines its plans to address any necessary revisions to the cyber security regulatory framework, and include a discussion of how the staff intends to ensure that this policy decision is reflected in the staff's review and approval of licensee cyber security plans. Finally, the staff should respond to the August 9, 2010 NERC letter by September 30, 2010, consistent with this direction in this policy decision. This response should be handled through the Commission correspondence process.

SECY, please track.

cc: EDO
OGC
SECY