POLICY ISSUE
INFORMATION

November 19, 2010 SECY-10-0153

FOR: The Commissioners

FROM: R. W. Borchardt
Executive Director for Operations

SUBJECT: CYBER SECURITY – IMPLEMENTATION OF THE COMMISSION'S DETERMINATION OF SYSTEMS AND EQUIPMENT WITHIN THE SCOPE OF TITLE 10 OF THE *CODE OF FEDERAL REGULATIONS*, SECTION 73.54

PURPOSE:

In the staff requirements memorandum (SRM), "CMWCO-10-0001 Regulation of Cyber Security at Nuclear Power Plants," dated October 21, 2010, the Commission determined as a matter of policy that the U.S. Nuclear Regulatory Commission's (NRC's) cyber security rule at Title 10 of the *Code of Federal Regulations* (10 CFR) Section 73.54, "Protection of Digital Computer and Communication Systems and Networks," should be interpreted to include structures, systems, and components (SSCs) in the balance of plant (BOP) that have a nexus to radiological health and safety at NRC-licensed nuclear power plants (NPPs). The purpose of this paper is to inform the Commission of the staff's implementation of the Commission's policy determination.

SUMMARY:

In the October 21, 2010, SRM, the Commission stated that the NRC's cyber security rule at 10 CFR 73.54 should be interpreted to include SSCs in the BOP that have a nexus to radiological health and safety. The staff determined that SSCs in the BOP that have a nexus to

CONTACT: Eric Lee, NSIR/DSP
(301) 415-8009

radiological health and safety are those that could directly or indirectly affect reactivity of an NPP, and are therefore within the scope of important-to-safety functions described in 10 CFR 73.54(a)(1). This information paper outlines the staff's short-term, intermediate, and long-term actions for implementing the Commission's interpretation concerning SSCs in the BOP. These include development of guidance in the form of a template licensees can use to supplement their cyber security plans, updating security and safety-related revisions to regulatory guides, and evaluation of the potential need for changes to NRC regulations. In addition, impacts on staffing requirements are discussed in terms of cyber security regulatory program and inspection related support.

BACKGROUND:

In January 2008, the Federal Energy Regulatory Commission (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. Order No. 706 specifically exempted "facilities regulated by the NRC" from these requirements. It was later determined that this exemption created a potential gap between NRC and FERC cyber security requirements as they apply to NPPs because the NRC staff interpreted the agency's cyber security regulation, 10 CFR 73.54, published in March 2009, to require the protection of digital systems that, if compromised, could directly or indirectly result in radiological sabotage.

The scope of systems under 10 CFR 73.54 includes systems associated with safety, important-to-safety, security, and emergency preparedness functions, as well as support systems and equipment that, if compromised, could adversely impact safety, security, or emergency preparedness functions. The staff did not consider many of the BOP SSCs to be within the scope of 10 CFR 73.54. Therefore, the staff believed that these BOP SSCs fell within the scope of the North American Electric Reliability Corporation's (NERC's) CIP standards.

On March 19, 2009, FERC issued Order No. 706-B to address this potential gap by clarifying that the BOP systems and equipment within an NPP that are not within the scope of 10 CFR 73.54 are subject to compliance with the CIP standards approved in Order No. 706. Order No. 706-B allowed nuclear facilities to seek exceptions from NERC's CIP standards on a case-by-case basis for those digital assets subject to the NRC's cyber security requirements.

In October 2009, the NRC staff briefed the Commission on NRC and NERC cyber security jurisdictional issues, future cyber security inspections at NRC-licensed NPPs, and the status of the memorandum of understanding (MOU) between the NRC and NERC. In December 2009, the NRC and NERC entered into an MOU addressing how NRC and NERC would cooperate on handling their respective authority over cyber security issues at NPPs. The NRC and NERC committed to cooperate in considering specific exception requests from NPPs in the December 2009 MOU.

NERC subsequently sent a letter to all NPPs, known as the “Bright-Line” Survey, requesting that, by June 24, 2010, all NPPs determine which of their SSCs were potentially subject to NERC CIP standards and which were potentially subject to NRC cyber security regulations. All NRC NPP licensees declared in their responses that the BOP SSCs, if compromised, affect reactivity and are important-to-safety. NRC NPP licensees further stated that for this reason, all BOP SSCs fall within the scope of the NRC’s cyber security regulations.

In a letter dated August 9, 2010, NERC informed the NRC that based on the responses to the Bright-Line Survey, 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. The conditions specified by NERC are that licensees notify the NRC by letter of all BOP SSCs licensees consider important-to-safety and submit a revised cyber security plan to the NRC for review and approval. In late August 2010, NERC sent a letter to all NRC NPP licensees stating these requirements. Each licensee sent the requested notification letter to the NRC and committed to update their cyber security plan to include BOP SSCs within their plans.

In the October 21, 2010, SRM, the Commission stated that the NRC’s cyber security rule at 10 CFR 73.54 should be interpreted to include SSCs in the BOP that have a nexus to radiological health and safety. The SRM directed NRC staff to take appropriate steps to immediately inform NRC licensees, NERC, and FERC of the Commission’s decision. The SRM also directed NRC staff to provide the Commission with an information paper discussing implementation of this decision, including any necessary revisions to the cyber security regulatory framework, any needed rulemakings or impacts on the development of an inspection process for cyber security.

DISCUSSION:

Under 10 CFR 73.54(a)(1), each licensee must provide high assurance that digital computer and communication systems and networks associated with the following are adequately protected against cyber attacks, up to and including the design-basis threat as described in 10 CFR 73.1: (1) safety-related and important-to-safety functions; (2) security functions; (3) emergency preparedness functions, including offsite communications; and (4) support systems and equipment that, if compromised, would adversely impact safety, security, or emergency preparedness functions.

The staff determined that SSCs in the BOP that have a nexus to radiological health and safety are those that could directly or indirectly affect reactivity of an NPP, and are therefore within the scope of important-to-safety functions described in 10 CFR 73.54(a)(1). The staff also determined that SSCs in the BOP are under licensee control and could be in the protected area or in the owner controlled area. The electrical distribution equipment out to the first inter-tie with the offsite distribution system would be subject to the NRC’s cyber security regulations. Based on this determination, the staff does not believe that there will be any SSCs in the BOP that will fall under NERC’s CIP standards. However, there may be some SSCs that are not subject to either NRC’s cyber security regulations or NERC’s CIP standards because these SSCs do not

directly or indirectly affect reactivity and do not affect grid reliability. Consistent with the MOA between NRC and FERC, the staff will continue to coordinate with FERC and NERC to share relevant operating experience and other related technical information on SSCs inside and beyond the scope of 10 CFR 73.54(a)(1).

The decision to include SSCs in the BOP within the scope of important-to-safety functions described in 10 CFR 73.54(a)(1) will ensure the programmatic cyber security requirements and associated security controls described in the licensees' cyber security plans apply to all digital systems and equipment that could directly or indirectly affect reactivity of an NPP. This includes establishment of an infrastructure at the NPPs that deters, detects and reacts to both internal and external cyber attacks. Licensee cyber security programs establish in procedures or other plant documents how responses to threat notifications regarding vulnerabilities against systems or equipment within the scope of 10 CFR 73.54(a)(1) received from a credible source are screened, evaluated and dispositioned. Specifically, licensees have committed in their cyber security plans that they will manage cyber risk through evaluation of threats and vulnerabilities to computer and control systems during the life cycle phases as documented in the Engineering Design Control, Configuration Management, Operating Experience and Corrective Action Program processes.

These credible sources may include cyber attacks against other systems in the plant not within the scope of 10 CFR 73.54(a)(1). We expect that an extent of condition review would be performed to evaluate those cyber security-related issues as potential precursors to issues impacting digital systems and equipment within the scope of 10 CFR 73.54(a)(1), and corresponding actions taken to put adequate protective measures in place. While the cyber security plans developed pursuant to 10 CFR 73.54 would not apply to these systems, in the absence of a separate program that would be applied, the extent of condition review would be performed in accordance with procedures that govern response to plant events for the identification, detection, and mitigation of cyber attacks. A discussion with the licensee representatives indicated the extent of condition review is part of their correction action program.

The staff developed an approach comprising short, intermediate, and long-term actions for implementing the Commission's interpretation concerning SSCs in the BOP. The details of the staff's implementation plan are discussed below.

Short-Term Actions:

As directed in the SRM, the staff took immediate actions to reach out to appropriate points of contact at FERC, NERC, and the Nuclear Energy Institute (NEI) as representatives for the nuclear power industry. The staff will follow this initial contact with a letter to each organization explaining the Commission's policy decision. These letters will be publicly available to ensure that external stakeholders are informed of this Commission policy and will be issued by the end of November 2010.

To facilitate the expeditious revision of already submitted cyber security plans, the staff will

develop guidance in the form of a template that licensees can utilize for their supplements. The template will include information on SSCs in the BOP that, if compromised, could affect NPP reactivity. This action will facilitate licensee compliance with NERC's request in its August 2010 letter that each licensee submit a revised cyber security plan to the NRC that includes all BOP SSCs considered important-to-safety. The staff plans to have the template developed and coordination with industry underway by early December 2010. The staff expects that all licensees, including those licensed under 10 CFR Part 52, will conform to the Commission policy and supplement their cyber security plans to include SSCs in the BOP.

Intermediate Actions:

The staff will update Regulatory Guide (RG) 5.71 "Cyber Security Programs for Nuclear Facilities" to clarify that digital systems and equipment in the BOP that, if compromised, could affect NPP reactivity are important-to-safety and within the scope of 10 CFR 73.54. Additionally, industry representatives have indicated that they will revise the cyber security plan template and guidance contained in NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6, and request NRC endorsement. As part of the update to RG 5.71, the staff will review the updates to NEI 08-09, Revision 6, and endorse it if it adequately incorporates the Commission's interpretations provided in the SRM. The staff will begin to revise RG 5.71 in the second quarter of Fiscal Year (FY) 2011. The staff anticipates that the process of revising RG 5.71 will take one year to complete from the commencement of this activity.

The staff will also identify and evaluate other security and safety-related regulatory guides associated with cyber security and will update them if necessary. For example, the staff will evaluate RG 5.69, "Guidance for the Application of the Radiological Sabotage Design-Basis Threat in the Design, Development, and Implementation of a Physical Security Protection Program that Meets 10 CFR 73.55 Requirements" (Safeguards Information), to ensure that cyber security adversary characteristics are adequately addressed. This will be done in parallel with the revisions to RG 5.71.

NRC staff will review the standing Memorandum of Agreement between the NRC and FERC for any needed updates to reflect the Commission's interpretations provided in the SRM. The staff will also review the existing MOU between the NRC and NERC for possible updates, including clarification on what is meant by "important-to-safety" in 10 CFR 73.54 as well as an update related to enforcement actions. Updates to the MOU will also detail responsibilities, communications between both parties, and information related to cyber security. These reviews will commence in the third quarter of FY 2011.

Finally, the staff will incorporate guidance into the cyber security inspection procedure currently under development for the review of cyber security protections and SSCs in BOP that have critical digital assets. The staff plans to complete the revisions to the inspection procedure by the end of 2011.

Long-Term Actions:

Once revisions have been made to Regulatory Guidance and cyber security plans that reflect the Commission Policy on the scope of SSCs covered by §73.54 and §73.1, consistent with normal practices, the staff will monitor the effectiveness of §73.54 through the inspection program and operating experience, and determine if any revisions should be pursued.

RESOURCES:

COORDINATION:

The Office of the General Counsel reviewed this information paper and has no legal objection. The Office of the Chief Financial Officer has reviewed this paper for resource implications and has no objections.

SRM COMWCO-10-001 "Regulation of Cyber Security at Nuclear Power Plants", was marked Official Use Only - Sensitive Internal Information. As a result, the staff response is marked the same until the staff is directed otherwise.

/RA by Martin J. Virgilio for/

R. W. Borchardt
Executive Director
for Operations

Long-Term Actions:

Once revisions have been made to Regulatory Guidance and cyber security plans that reflect the Commission Policy on the scope of SSCs covered by §73.54 and §73.1, consistent with normal practices, the staff will monitor the effectiveness of §73.54 through the inspection program and operating experience, and determine if any revisions should be pursued.

RESOURCES:

COORDINATION:

The Office of the General Counsel reviewed this information paper and has no legal objection. The Office of the Chief Financial Officer has reviewed this paper for resource implications and has no objections.

SRM COMWCO-10-001 "Regulation of Cyber Security at Nuclear Power Plants", was marked Official Use Only - Sensitive Internal Information. As a result, the staff response is marked the same until the staff is directed otherwise.

/RA by Martin J. Virgilio for/

R. W. Borchardt
Executive Director
for Operations

ADAMS ACCESSION NO.: ML103490344 (W201000226; EDATS: SECY-2010-0503)

OFFICE	NSIR/DSP/ISCPB	NSIR/DSP/ISCPB/BC	NSIR/DSP	NSIR/DSO	QTE
NAME	E. Lee	C. Erlanger	D. Huyck for / R. Correia	P. Holahan	K. Azariah-Kribbs
DATE	11/10/10	11/10/10	11/12/10– by Email	11/10 /10 – by Email	11/5/10 – by Email
OFFICE	NRO	NRR	OGC	NSIR	OCFO
NAME	L. Dudes for/ M. Johnson	P. Holahan for/ E. Leeds	N. St. Amour for/ M. Young	S. Abraham	P. Wagner for/ J. Dyer
DATE	11/10/10 – by Email	11/10/10 – by Email	11/10/10 – by Email	11/10/10 – by Email	11/12/10 – by Email
OFFICE	NSIR	OEDO			
NAME	J. Wiggins	R. W. Borchardt			
DATE	11/12/10 – by Email	11/19/2010			

OFFICIAL RECORD COPY