EDO Principal Correspondence Control

FROM: DUE: 07/13/10 EDO CONTROL: G20100398
DOC DT: 06/18/10
FINAL REPLY:

Marvin S. Fertel
Nuclear Energy Institute (NEI)

TO:

Chairman Jaczko

FOR SIGNATURE OF : ** PRI ** CRC NO: 10-0280

Chairman Jaczko

DESC:

Oversight and Inspection of Cyber Security Requirements at the U.S. Nuclear Power Plants (EDATS: SECY-2010-0329)

ROUTING:

Borchardt
Weber
Virgilio
Ash
Mamish
OGC/GC
Leeds, NRR
Johnson, NRO
Burns, OGC
Bagley, OEDO

DATE: 06/23/10

ASSIGNED TO: CONTACT:

NSIR Wiggins

SPECIAL INSTRUCTIONS OR REMARKS:

EDATS

Electronic Document and Action Tracking System

EDATS Number: SECY-2010-0329 **Source:** SECY

General Information

Assigned To: NSIR
OEDO Due Date: 7/13/2010 11:00 PM
Other Assignees:
SECY Due Date: 7/15/2010 11:00 PM
Subject: Oversight and Inspection of Cyber Security Requirements at the U.S. Nuclear Power Plants
Description:

CC Routing: NRR; NRO; OGC
ADAMS Accession Numbers - Incoming: NONE
Response/Package: NONE

Other Information

Cross Reference Number: G20100398, LTR-10-0280
Staff Initiated: NO
Related Task:
Recurring Item: NO
File Routing: EDATS
Agency Lesson Learned: NO
OEDO Monthly Report Item: NO

Process Information

Action Type: Letter
Priority: Medium
Sensitivity: None
Signature Level: Chairman Jaczko
Urgency: NO
Approval Level: No Approval Required
OEDO Concurrence: YES
OCM Concurrence: NO
OCA Concurrence: NO
Special Instructions:

Document Information

Originator Name: Marvin S. Fertel
Date of Incoming: 6/18/2010
Originating Organization: NEI
Document Received by SECY Date: 6/23/2010
Addressee: Chairman Jaczko/J. Wellinghoff, FERC
Date Response Requested by Originator: NONE
Incoming Task Received: Letter

OFFICE OF THE SECRETARY
CORRESPONDENCE CONTROL TICKET

Date Printed: Jun 22, 2010 15:43

PAPER NUMBER:	LTR-10-0280	**LOGGING DATE:**	06/22/2010
ACTION OFFICE:	EDO		
AUTHOR:	Marvin Fertel		
AFFILIATION:	NEI		
ADDRESSEE:	Gregory Jaczko		
SUBJECT:	Oversight and inspection of Cyber Security Requirements at U.S. Nuclear Power Plants.....Proj #689		
ACTION:	Signature of Chairman		
DISTRIBUTION:	RF, OGC, SECY to Ack		
LETTER DATE:	06/18/2010		
ACKNOWLEDGED	No		
SPECIAL HANDLING:	Made publicly available in ADAMS via EDO/DPC		
NOTES:			
FILE LOCATION:	ADAMS		
DATE DUE:	07/15/2010	**DATE SIGNED:**	

EDO --G20100398

NUCLEAR ENERGY INSTITUTE

Marvin S. Fertel
PRESIDENT AND
CHIEF EXECUTIVE OFFICER

June 18, 2010

The Honorable Gregory B. Jaczko
Chairman
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001

The Honorable Jon Wellinghoff
Chairman
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

Subject: Oversight and Inspection of Cyber Security Requirements at U.S. Nuclear Power Plants

Project Number: 689

Dear Chairmen:

The owners/operators of the nation's 104 operating commercial nuclear power reactors have already implemented significant measures to protect their facilities against cyber attacks. The nuclear industry is also committed to implementing additional measures to satisfy the new rules and regulations which have been the focus of numerous discussions between the U.S. Nuclear Regulatory Commission (NRC), the Federal Energy Regulatory Commission (FERC), and the North American Electric Reliability Corporation (NERC). Successful implementation, however, is dependent on having clear regulatory requirements and appropriate and stable guidance. The purpose of the letter is to recommend a clear path forward to assure effective implementation of cyber security measures.

From the nuclear industry perspective it is clear that NRC's responsibility is to protect public health and safety. The role of FERC/NERC is to ensure a reliable bulk power system. In this regard, on January 18, 2008 FERC issued Order No. 706 which approved eight Critical Infrastructure Protection (CIP) Reliability Standards containing cyber security requirements. This order exempted NRC-regulated facilities on the basis that adequate cyber protection measures were embedded in NRC regulations. At the same time, NRC was collecting public comments on its proposed cyber security regulation. In the April 8, 2008 joint meeting of the commissioners from NRC and FERC, statements were made that the NRC cyber security requirements would not extend to power continuity systems. These statements left a perceived gap in protection and FERC issued a revised order (Order 706-B) on March 19, 2009 that removed the exemption. The NRC issued its final cyber security regulation on March 27, 2009.

1776 I Street, NW | Suite 400 | Washington, DC | 20006-3708 | P: 202.739.8125 | F: 202. 533.0134 | msf@nei.org | www.nei.org

This year, in a similar joint meeting held on March 16, 2010, the commissioners were told there is an overlap between the revised FERC order and NRC rule.

Dual regulation at any of our facilities is at best complex and challenging with respect to licensee implementation and oversight and inspection by regulators and in this case, as described below, we do not believe it is necessary to protect public health and safety or the integrity of the electricity grid.

FERC Order 706 approved CIPS prepared by NERC which "provide a comprehensive set of requirements to protect the Bulk-Power System from malicious cyber attack." From the nuclear industry perspective, FERC is imposing the implementation of these standards to ensure that a cyber event at a nuclear facility does not cause a disturbance to the grid. For this to occur, the cyber attack would have to impact a digital asset on a system or component that could cause the nuclear reactor to shut down, or trip, and disrupt the flow of electricity to the grid.

From an NRC perspective, that same trip is a reactivity event that can challenge safe shutdown of the reactor. In this regard, NRC does have specific regulatory requirements in place, such as technical specifications and the maintenance rule to ensure that such trips do not occur due to equipment exceeding operating limits or maintenance issues. These regulatory requirements are applicable to any equipment that could cause a reactor transient, including power continuity systems.

At issue now is whether the NRC cyber regulation applies to such balance of plant equipment. While we have not seen any information from the NRC or FERC that defines precisely what digital assets are covered by which requirements, we understand NERC is now conducting workshops to determine where the line is drawn.

However, the NRC's cyber security requirements in 10 CFR 73.54(a)(1) define the scope of equipment as follows:

> *(a) Each licensee subject to the requirements of this section shall provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in § 73.1.*
>
> *(1) The licensee shall protect digital computer and communication systems and networks associated with:*
>
> *(i) Safety-related and important-to-safety functions;*
>
> *(ii) Security functions;*
>
> *(iii) Emergency preparedness functions, including offsite communications; and*

(iv) Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

We believe the "important to safety functions" scoping criterion encompasses continuity of power system digital assets that, if compromised, can cause a plant to trip. What makes them important to safety is the fact that a plant trip is a reactivity event that challenges safe shutdown. Therefore, we will have appropriate cyber security controls on these digital assets. The plant trip also has the potential to disturb the bulk power system which is FERCs concern. Whether the plant trips because equipment operates beyond its design limit or fails because of a cyber attack does not alter the net result. Thus, in our view, the overlap that exists between the two regulatory requirements is the critical digital assets on systems or components that could cause a plant trip.

The most effective and efficient resolution of this issue is the determination that the scope of 10 CFR 73.54 includes continuity of power systems, which overlaps the FERC CIP scope. Therefore, NRC power reactor licensees may be exempted from the FERC order, and the oversight and inspection of the implementation of cyber security requirements should be conducted by the NRC. We strongly believe that the commissions should affirm this position in the near term so that implementation can proceed expeditiously.

We would be pleased to discuss this matter further with both commissions. Please contact me if you have any questions.

Sincerely,

Marvin S. Fertel

c: Commissioner Philip D. Moeller, Federal Energy Regulatory Commission
Commissioner Marc L. Spitzer, Federal Energy Regulatory Commission
Commissioner John R. Norris, Federal Energy Regulatory Commission
Commissioner Kristine L. Svinicki, U.S. Nuclear Regulatory Commission
Commissioner William D. Magwood, U.S. Nuclear Regulatory Commission
Commissioner George Apostolakis, U.S. Nuclear Regulatory Commission
Commissioner William C. Ostendorff, U.S. Nuclear Regulatory Commission
Mr. R. William Borchardt, U.S. Nuclear Regulatory Commission
Mr. Martin Virgilio, U.S. Nuclear Regulatory Commission
Mr. James T. Wiggins, U.S. Nuclear Regulatory Commission
NRC Document Control Desk