PR 50, 72 and 73
(71FR62663)

(2)

DOCKETED
USNRC

December 11, 2006 (10:44am)

OFFICE OF SECRETARY
RULEMAKINGS AND
ADJUDICATIONS STAFF

December 7, 2006

Ms. Annette Vietti-Cook
Office of the Secretary
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: *Comments on RIN 3150-AG63, Power Reactor Security Requirements,*

Dear Ms. Vietti-Cook:

As a recognized expert in the area of cyber security of industrial control systems, including those used in commercial nuclear power plants, I have enclosed my comments on the proposed rulemaking. I do have substantial background in nuclear power having managed the EPRI Nuclear Plant Instrumentation and Diagnostics Program for 5 years. I have included the specific item from the rulemaking in Melior 9 and my comments in Times New Roman 12.

P. 62667- 6. *Cyber-security requirements.* This proposed rule would contain more detailed programmatic requirements for addressing cyber security at power reactors, which build on the requirements imposed by the February 2002 order. The proposed cyber-security requirements are designed to be consistent with ongoing industry cybersecurity efforts.

Ongoing industry efforts include ISA SP99 which specifically includes nuclear plants, NERC CIP which specifically exclude nuclear power plants, and NEI-0404. Of these three efforts, only ISA SP99 is specifically addressing industrial control systems including those used in commercial nuclear power plants.

P.62667 - 10. *Security Program Implementation insights.* The proposed rule would impose new enhancements identified from implementation of the security orders, review of site security plans, and implementation of the enhanced baseline inspection program and force-on- force exercises. These new requirements would include changes to specifically require that the central alarm station (CAS) and secondary alarm station (SAS) have functionally equivalent capabilities such that no single act can disable the key functions of both CAS and SAS. The proposed additions would also include requirements for new reactor licensees to position the SAS within the protected area, add bullet resistance and limit the visibility into SAS. Proposed additions also require uninterruptible backup power supplies for detection and assessment equipment, "video-capture" capability, and qualification requirements for drill and exercise controllers.

CAS and SAS may also have cyber connections. There are no requirements to address any possible cyber connections.

P. 62670 - Requirements for CAS and SAS To Have Functionally Equivalent Capabilities Such That No Single Act Can Disable the Function of CAS and SAS

Cyber security is not identified.

P.62670 - 1. What insights and estimates can stakeholders provide on the feasibility, costs, and time necessary to implement the proposed rule's changes to existing alarm stations, supporting systems, video systems, and cyber security?

The feasibility associated with establishing a cyber security program for industrial control systems has been demonstrated by various electric utilities (fossil power plants,

Template = SECY-067

SECY-02

substations, and control centers) chemical plants, refineries, and other facilities with systems similar, if not identical, to those used in the balance-of-plant in commercial nuclear plants. The time and cost necessary to implement a control system cyber security program is dependent on the scope and findings. Currently, there are minimal technologies available to electronically secure the field devices used in power plant or control yard facilities. However, there are programmatic approaches developed by the ISA 99 Control System Cyber Security committee and NIST 800-82 that can be implemented now to augment the NEI-0404 recommendations.

P.62670 2. Are there any actions that should be considered, such as authorizing alternative measures, exemptions, extended implementation schedules, etc. that would allow the NRC to mitigate any unnecessary regulatory burden created by these requirements?
There are no feasible reasons for not immediately implementing a comprehensive control system cyber security program including establishing control system security policies and procedures and performing a comprehensive vulnerability/risk assessment. The longer these actions are deferred, the longer the nuclear plants will be at risk.

P.62835-Table 7 (j)(3)ii) Provide required training to include simulator training for the operations response to security events (e.g., loss of ultimate heat sink) for nuclear power reactor personnel in accordance with site procedures to ensure the operational readiness of personnel commensurate with assigned duties and responsibilities.
Required training should include identification of potential cyber threats and appropriate remedial actions.

If you have any questions, please contact me. Thank you for your consideration,

Joe Weiss, PE, CISM
Executive Consultant, KEMA, Inc.
(408) 253-7934
(408) 832-5396 Cell
joe.weiss@kema.com

From: Evangeline Ngbea
To: SECY
Date: Mon, Dec 11, 2006 8:29 AM
Subject: Fwd: Comment letter on Power Reactor Security Requirements Proposed Rule

>>> Carol Gallagher 12/08/2006 11:17 AM >>>
Van,

Attached for docketing is a comment letter on the above noted proposed rule from Joe Weiss that I received via the rulemaking website on December 7, 2006.

His address is:

Joe Weiss
10029 Oakleaf Place
Cupertino CA 95014
joe.weiss@kema.com

Carol

Mail Envelope Properties (45798FFC.41A : 5 : 35764)

Subject:	Comment letter on Power Reactor Security Requirements Proposed Rule
Creation Date	12/08/2006 11:17:00 AM
From:	Carol Gallagher
Created By:	CAG@nrc.gov

Recipients
nrc.gov
TWGWPO01.HQGWDO01
ESN (Evangeline Ngbea)

Post Office	**Route**
TWGWPO01.HQGWDO01	nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	938	12/08/2006 11:17:01 AM
TEXT.htm	719	
1785-0003.doc	28160	12/08/2006 11:12:56 AM

Options

Expiration Date:	None
Priority:	Standard
ReplyRequested:	No
Return Notification:	None
Concealed Subject:	No
Security:	Standard

Junk Mail Handling Evaluation Results
Message is not eligible for Junk Mail handling
Message is from an internal sender

Junk Mail settings when this message was delivered
Junk Mail handling disabled by User
Junk Mail handling disabled by Administrator
Junk List is not enabled
Junk Mail using personal address books is not enabled
Block List is not enabled