MITSUBISHI HEAVY INDUSTRIES, LTD.
16-5, KONAN 2-CHOME, MINATO-KU
TOKYO, JAPAN

March 31, 2009

Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Attention: Mr. Jeffrey A. Ciocco

Docket No. 52-021
MHI Ref: UAP-HF-09129

Subject: MHI's Responses to US-APWR DCD RAI No.277-2095 Revision 1

Reference: 1) "Request for Additional Information 277-2095 Revision 1 SRP Section: 07-09 – Data Communication Systems, Application Section: 07.09, dated 3/12/2009

With this letter, Mitsubishi Heavy Industries, Ltd. ("MHI") transmits to the U.S. Nuclear Regulatory Commission ("NRC") a document as listed in Enclosures.

Enclosure 1 and 2 are the responses to RAIs contained within References 1.

The RAI Response is being submitted in two versions. One version (Enclosure 1) includes certain information, designated pursuant to the Commission guidance as sensitive unclassified non-safeguards information, referred to as security-related information ("SRI"), that is to be withheld from public disclosure under 10 CFR 2.390. The information that is SRI is identified by brackets. The second version (Enclosure 2) omits the SRI and is suitable for public disclosure. In the public version, the SRI is replaced by the designation "[Security-Related Information - Withheld Under 10 CFR 2.390]".

Please contact Dr. C. Keith Paulson, Senior Technical Manager, Mitsubishi Nuclear Energy Systems, Inc. if the NRC has questions concerning any aspect of the submittals. His contact information is below.

Sincerely,

Y. Ogata

Yoshiki Ogata,
General Manager- APWR Promoting Department
Mitsubishi Heavy Industries, LTD.

Enclosures:

1. Responses to Request for Additional Information No.277-2095 Revision 1 (SRI included version)

D081
NRO

2. Responses to Request for Additional Information No.277-2095 Revision 1
(SRI excluded version)

CC: J. A. Ciocco
C. K. Paulson

Contact Information
C. Keith Paulson, Senior Technical Manager
Mitsubishi Nuclear Energy Systems, Inc.
300 Oxford Drive, Suite 301
Monroeville, PA 15146
E-mail: ck_paulson@mnes-us.com
Telephone: (412) 373-6466

Enclosure 2

UAP-HF-09129
Docket No. 52-021

Responses to Request for Additional Information No.277-2095
Revision 1

March 2009

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

3/31/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO. 277-2095 REVISION 1**
SRP SECTION:	**07.09 DATA COMMUNICATION SYSTEMS**
APPLICATION SECTION:	**07.09 DATA COMMUNICATION SYSTEMS**
DATE OF RAI ISSUE:	**3/12/2009**

QUESTION NO.: 07-09-8455
Demonstrate how the guidance of NUREG/CR-6847 was incorporated in the development of the Critical Digital Asset (CDA) assessment requirements.

Security-Related Information - Withheld Under 10 CFR 2.390

ANSWER:
NUREG/CR-6847 was written for operating plants. The level of detail required about the assessment process, as described in the NUREG is not available (including walk downs and connectivity assessments) in MUAP-08003, "US-APWR Cyber Security Program".

However, MUAP-08003 already incorporates the approach of the cyber security assessment from NUREG/CR-6847. Section 3.8 and Figure 3.8-1 describes the assessment and risk management processes which are equivalent to that of NUREG/CR-6847.

Impact on DCD

There is no impact on the DCD.

Impact on COLA
There is no impact on the COLA.

Impact on PRA
There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

3/31/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO. 277-2095 REVISION 1**
SRP SECTION:	**07.09 DATA COMMUNICATION SYSTEMS**
APPLICATION SECTION:	**07.09 DATA COMMUNICATION SYSTEMS**
DATE OF RAI ISSUE:	**3/12/2009**

QUESTION NO.: 07-09-8456

Describe what security features are incorporated into the design of the PSMS and PCMS to mitigate vulnerabilities that can be exploited in the design.

Security-Related Information - Withheld Under 10 CFR 2.390

ANSWER:

Section 5.1 of MUAP-08003 describes the key cyber security aspects and security capabilities for the PSMS. As described in Section 5.1 of MUAP-08003, detailed descriptions of the security features of the PSMS design are described as following reports;

- The cyber security aspects of the digital systems/equipment life cycle for the PSMS basic software are described in Section 6.1.6 of Topical Report MUAP-07005, "Safety System Digital Platform MELTAC". For example, Section 6.1.6 describes measures to ensure there is no unintended code included in the PSMS software during the process of software development.

- The cyber security aspects of the digital systems/equipment life cycle for the PSMS application software is generally described in Section 6.4.3 of Topical Report MUAP-07004, "Safety I&C System Description and Design Process".
- Additional details of the application software cyber security aspects are described in each section of Technical Report MUAP-07017, "Software Program Manual".

Section 5.2 of MUAP-08003 describes the key cyber security aspects and security capabilities for the PCMS.

For example, Section 5.2 requires that all applications, binaries and supporting files transferred into the PCMS development environment be scanned for viruses, worms or other forms of malicious code prior to installation into the test environment utilizing a virus scanning workstation that has an up-to-date signature set.

Impact on DCD
There is no impact on the DCD.

Impact on COLA
There is no impact on the COLA.

Impact on PRA
There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

3/31/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO. 277-2095 REVISION 1**
SRP SECTION:	**07.09 DATA COMMUNICATION SYSTEMS**
APPLICATION SECTION:	**07.09 DATA COMMUNICATION SYSTEMS**
DATE OF RAI ISSUE:	**3/12/2009**

QUESTION NO.: 07-09-8457
Provide additional information demonstrating the adequacy of the cyber security defensive strategy described in Section 4.0 of the US-APWR Cyber Security Program, MUAP-08003-P(R0).

Security-Related Information - Withheld Under 10 CFR 2.390

ANSWER:
Section 1.1 of MUAP-08003 describes the purpose of this report;

> "This program document is intended to form the basis of specific cyber security management procedures which are implemented by each organization (MHI, suppliers/partners, COL Applicant). The actual implementation of the program at the COL facility, and the result of the

final detail design for that facility, would be the subject of the COL Applicant's plant implementing procedures. This document describes the key defensive strategies of the US-APWR Cyber Security Program. However, cyber threats are continuously evolving as persons with malicious intent find new ways to breach security barriers. To address this concern, the program also includes programmatic requirements for ongoing periodic audit and assessment of the effectiveness of the program, including ongoing assessment of cyber threats. Ongoing enhancements to the plant's cyber security defenses are expected. Specific organizational procedures shall be updated, as necessary, to reflect these ongoing programmatic changes."

This technical report made the commitment that PSMS and PCMS systems and components shall be designed to meet the cyber security defensive strategies described in this report. The actual design including the allowed and disallowed protocols, methods used to prevent the disallowed protocols from being used on the network, the unidirectional firewall, and the configuration of the DMZ will be designed using applicable codes and standards, good industry practice such as NEI 04-04, and state of the art technology to mitigate the cyber threat.

Therefore, more detailed design information of the PSMS and PCMS systems and components has not yet been developed, and is not available in this report.

Impact on DCD
There is no impact on the DCD.

Impact on COLA
There is no impact on the COLA.

Impact on PRA
There is no impact on the PRA.