November 2, 2012

Mr. Thomas Saporito, Senior Consultant
Saprodani Associates
6701 Mallards Cove Road, Apartment 28H
Jupiter, Florida 33458

Dear Mr. Saporito:

I am responding to your petition dated July 30, 2012, addressed to the Office of the Secretary of the Commission, U.S. Nuclear Regulatory Commission (NRC), which was referred to the Office of Nuclear Reactor Regulation (NRR) pursuant to Section 2.206 of Title 10 of the *Code of Federal Regulations* (10 CFR 2.206).

Management Directive (MD) 8.11, which is publicly available (Agencywide Documents and Management System (ADAMS) Accession No. ML041770328) describes the NRC's review process for 10 CFR 2.206 petitions.

The petition was filed under 10 CFR 2.206 and requested enforcement action against all NRC licensees as a result of a July 30, 2012, Bloomberg News Agency broadcast which reported that cyber hackers had succeeded in breaking into the computer network of an NRC-licensed nuclear plant. Specifically, you requested that:

1. The NRC take escalated enforcement action against all NRC licensees and suspend, or revoke the NRC license(s) granted to the licensee(s) for operation of any nuclear reactor or facility.

2. The NRC issues a notice of violation with a proposed civil penalty against the licensee(s) in the total amount of $100,000.00 (One-Hundred Thousand) dollars.

3. The NRC issues a confirmatory order to the licensee(s) requiring the licensee(s) to take their nuclear reactors and/or nuclear facilities to a cold-shutdown mode of operation until such time as:
   - The licensee completes an "independent" assessment to understand fully and correct the potential and/or realized cyber security threat posed by outside organizations;
   - The licensee completes a comprehensive evaluation of all nuclear safety related plant equipment and components which may be otherwise modified and/or operated by remote means via Internet access;
   - The licensee completes, identifies and removes any and all Internet access points to all nuclear safety related plant equipment and/or components; and
   - The licensee completes and "independent" safety-assessment through a 3rd party contractor to review all plant nuclear safety related equipment and/or components – to ensure that such nuclear safety related systems and/or components are not accessible by an unauthorized entity via the Internet."

On July 31, 2012, the NRR Senior Project Manager and 10 CFR 2.206 Coordinator, Ms. Tanya Mensah, contacted you by e-mail to describe the 10 CFR 2.206 process and to provide you with a copy of MD 8.11. Ms. Mensah also offered you an opportunity to address the NRC's Petition Review Board (PRB). You accepted the offer and requested an opportunity, in person, to address the PRB during an NRC public meeting.

PRB's Decision Regarding The Request For Immediate Action

On August 27, 2012, the PRB met internally to discuss the request for immediate action within your petition. MD 8.11, Part III.A.1, "Schedule," states that the PRB meeting may be held sooner if staff decisions are required on short-term, immediate actions. Although you did not characterize Item 3 in your petition as immediate, the PRB treated the request to require the licensee(s) to take their nuclear reactors and/or nuclear facilities to a cold-shutdown mode of operation, as an immediate action.

During the August 27th internal meeting, the PRB discussed that in accordance with 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," each licensee shall protect digital computer and communication systems and networks associated with (1) safety-related and important-to-safety functions; (2) security functions; (3) emergency preparedness; and (4) support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions. With regard to the information referenced in the Bloomberg news article, there was no indication that any digital computer, communication system, or network subject to the requirements of 10 CFR 73.54 was impacted. In addition, NRC licensees subject to the requirements of 10 CFR 73.54 have submitted cyber security plans and an implementation schedule, which the NRC staff has reviewed and approved.

Therefore, the PRB determined, in accordance with MD 8.11, that you did not provide sufficient information that any digital computer, communication systems, or networks associated with 10 CFR 73.54 has been or will be adversely impacted as a result of a cyber attack. In addition, the PRB did not have any information to conclude that there was an immediate safety concern at any NRC-licensed facilities. On that basis, the PRB denied the request for immediate action.

On September 5, 2012, Ms. Mensah informed you in an e-mail of the PRB's decision to deny the request for immediate action.

On September 10, 2012, you addressed the PRB during an NRC public meeting (ADAMS Accession No. ML12228A529) and provided supplemental information in support of your petition request. Your presentation materials included meeting handouts (ADAMS Accession No. ML12256A746) and videos, which you provided to the petition manager on a compact disc (CD). Video files cannot be declared as an official NRC agency record in ADAMS; therefore, the videos are publicly available on CD in the NRC Public Document Room (ADAMS Accession No. ML12256A739). The transcript from the public meeting is also publically available (ADAMS Accession No. ML12263A002).

During the public meeting, you discussed the Florida, Power & Light Smart Grid and the use of Smart devices; however, this issue relates to an area of concern (grid security and reliability), which is outside the purview of NRC regulations.

PRB's Initial Recommendation

On October 1, 2012, the PRB met and discussed the remaining requests within your petition, as supplemented on September 10, 2012.

Your petition requested that the NRC take escalated enforcement action against all NRC licensees and suspend, or revoke the NRC license(s) granted to the licensee(s) for operation of any nuclear reactor or facility. In addition, you requested that the NRC issue a notice of violation with a proposed civil penalty against the licensee(s) in the total amount of $100,000.00 (One-Hundred Thousand) dollars.

In accordance with MD 8.11, Part III, C.1, "Criteria For Reviewing Petitions Under 10 CFR 2.206," these requests do not meet the criteria for review on the basis that the petition, as supplemented, failed to provide sufficient facts to warrant further inquiry.

During the September 10, 2012, public meeting, I, in my role as PRB Chairman, asked you to clarify if your request for enforcement was limited to operating reactor licensees. Your response was that the petition is applicable to all NRC licensees (as stated in the petition) including as examples: nuclear fuel reprocessing facilities; facilities that make nuclear fuel rods; and hospitals. However, your petition, as supplemented on September 10, 2012, only contained general assertions of safety and cyber security concerns at these types of facilities and did not provide specific facts relating to NRC-regulated activities. Therefore, the PRB determined that the scope of your petition (as applicable to NRC licensees that do not hold operating reactor licenses) does not meet the criteria for review on the basis that the petition, as supplemented, failed to provide sufficient facts to warrant further inquiry, as described in MD 8.11, Part III, C.1.

Your petition also requested that the NRC issue a confirmatory order to the licensee(s) requiring the licensee(s) to take their nuclear reactors and/or nuclear facilities to a cold-shutdown mode of operation until such time as:

- The licensee completes an "independent" assessment to understand fully and correct the potential and/or realized cyber security threat posed by outside organizations;
- The licensee completes a comprehensive evaluation of all nuclear safety related plant equipment and components which may be otherwise modified and/or operated by remote means via Internet access;
- The licensee completes, identifies and removes any and all Internet access points to all nuclear safety related plant equipment and/or components; and
- The licensee completes and "independent" safety-assessment through a 3rd party contractor to review all plant nuclear safety related equipment and/or components – to ensure that such nuclear safety related systems and/or components are not accessible by an unauthorized entity via the Internet.

In accordance with MD 8.11, Part III, C.2, "Criteria For Rejecting Petitions under 10 CFR 2.206," these requests meet the criteria for rejection on the basis that the issues raised in the petition, as supplemented, have already been reviewed, evaluated, and resolved by the NRC. The petition, as supplemented, did not provide information that any computer, communication system, or network subject to the requirements of 10 CFR 73.54, for any NRC licensees, has been impacted. On a generic basis, NRC licensees subject to the requirements of 10 CFR 73.54 have submitted cyber security plans and an implementation schedule, which the NRC staff has reviewed and approved. The NRC will begin cyber security inspections in 2013, which will also address your request for the licensee(s) to complete an independent safety-assessment through a 3rd party contractor. Therefore, for commercial operating reactors, the petitioner raises issues that have already been reviewed, evaluated, and resolved by the NRC, as described in MD 8.11, Part III, C.2.

On October 2, 2012, the NRR petition manager, Ms. Mensah, informed you of the PRB's initial recommendation and requested that you respond by October 9, 2012, if you wanted a second opportunity to address the PRB. Furthermore, Ms. Mensah stated in her e-mail that if you did not respond by October 9, 2012, the PRB's initial recommendation would become final.

PRB's Final Recommendation

Since you did not provide a response to Ms. Mensah, as requested, the PRB's initial recommendation, as described above, is now the final recommendation.

For additional information, a backgrounder regarding the NRC's cyber security requirements and applicable regulations for licensees is available on the NRC's public website (http://www.nrc.gov). You can access the backgrounder directly from the NRC's public website by selecting the following options: (Home > NRC Library > Document Collections > Fact Sheets > Backgrounder on Cyber Security).

In addition, in January 2010, the NRC published Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," (ADAMS Accession No. ML090340159) that provides comprehensive guidance to licensees and applicants for licenses on an acceptable way to meet the requirements of 10 CFR 73.54. The guidance includes recommended best practices from such organizations as the International Society of Automation, the Institute of Electrical and Electronics Engineers, and the National Institute of Standards and Technology, as well as guidance from the U.S. Department of Homeland Security.

Thank you for bringing these issues to the attention of the NRC.

Sincerely,

/RA/

Ho Nieh, Division Director
Division of Inspection and Regional Support
Office of Nuclear Reactor Regulation

cc/w incoming 2.206 Petition

In accordance with MD 8.11, Part III, C.2, "Criteria For Rejecting Petitions under 10 CFR 2.206," these requests meet the criteria for rejection on the basis that the issues raised in the petition, as supplemented, have already been reviewed, evaluated, and resolved by the NRC. The petition, as supplemented, did not provide information that any computer, communication system, or network subject to the requirements of 10 CFR 73.54, for any NRC licensees, has been impacted. On a generic basis, NRC licensees subject to the requirements of 10 CFR 73.54, have submitted cyber security plans and an implementation schedule, which the NRC staff has reviewed and approved. The NRC will begin cyber security inspections in 2013, which will also address your request for the licensee(s) to complete an independent safety-assessment through a 3rd party contractor. Therefore, for commercial operating reactors, the petitioner raises issues that have already been reviewed, evaluated, and resolved by the NRC, as described in MD 8.11, Part III, C.2.

On October 2, 2012, the NRR petition manager, Ms. Mensah, informed you of the PRB's initial recommendation and requested that you respond by October 9, 2012, if you wanted a second opportunity to address the PRB. Furthermore, Ms. Mensah stated in her e-mail that if you did not respond by October 9, 2012, the PRB's initial recommendation would become final.

PRB's Final Recommendation

Since you did not provide a response to Ms. Mensah, as requested, the PRB's initial recommendation, as described above, is now the final recommendation.

For additional information, a backgrounder regarding the NRC's cyber security requirements and applicable regulations for licensees is available on the NRC's public website (http://www.nrc.gov). You can access the backgrounder directly from the NRC's public website by selecting the following options: (Home > NRC Library > Document Collections > Fact Sheets > Backgrounder on Cyber Security).

In addition, in January 2010, the NRC published Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," (ADAMS Accession No. ML090340159) that provides comprehensive guidance to licensees and applicants for licenses on an acceptable way to meet the requirements of 10 CFR 73.54. The guidance includes recommended best practices from such organizations as the International Society of Automation, the Institute of Electrical and Electronics Engineers, and the National Institute of Standards and Technology, as well as guidance from the U.S. Department of Homeland Security.

Thank you for bringing these issues to the attention of the NRC.

Sincerely,
/RA/
Ho Nieh, Division Director
Division of Inspection and Regional Support
Office of Nuclear Reactor Regulation

cc/w incoming 2.206 Petition
Distribution via Listserv

DISTRIBUTION: (G20120557/EDATS: SECY-2012-0392)

PUBLIC	RidsEdoMailCenter	NGarcia-Santos, NMSS
Resource	RidsNrrOd Resource	RidsOgcRp Resource
RidsNrrDorl Resource	RidsOpaMail Resource	RidsNrrMailCenter Resource
RidsOcaMailCenter Resource		RidsRgn4MailCenter Resource
CSafford, OGC	NColeman, OE	RidsNrrDpr Resource
JSebrosky, NRR	JDeCicco, FSME	TMensah, NRR
PPederson, NSIR	MFernandez, NSIR	
LHowell, RIV	TMossman, NRR	

ADAMS Package No. ML12283A155 **Incoming – ML12215A022**
Letter - ML12283A152 **Public Meeting Notice - ML12228A529**
Public Meeting Handouts- ML12256A746 **Public Meeting Video- ML12256A739**
Public Meeting Transcript- ML12263A002 ***e-mail concurrence**

OFFICE	DPR/PGCB/PM	DPR/PGCB/LA	DPR/PGCB/BC	RIV/RCB/BC	DE/EICB/BC	NSIR/DSO/RSOB/BC	DIRS/D
NAME	TMensah	CHawes	DPelton	LHowell*	JThorp (TMossman for)*	RAlbert*	HNieh
DATE	10/11 /12	10/11/12	10/ 11 /12	10/ 11 /12	10/11 /12	10/15 /12	10/ 2 /12

OFFICIAL RECORD COPY