



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

March 4, 2011

Mr. Michael J. Pacilio
President and Chief Nuclear Officer
Exelon Nuclear
4300 Winfield Road
Warrenville, IL 60555

SUBJECT: BRAIDWOOD STATION, UNITS 1 AND 2; BYRON STATION, UNIT NOS. 1 AND 2; CLINTON POWER STATION, UNIT NO. 1; DRESDEN NUCLEAR POWER STATION, UNITS 2 AND 3; LASALLE COUNTY STATION, UNITS 1 AND 2; LIMERICK GENERATING STATION, UNITS 1 AND 2; OYSTER CREEK NUCLEAR GENERATING STATION; PEACH BOTTOM ATOMIC POWER STATION, UNITS 2, AND 3; QUAD CITIES NUCLEAR POWER STATION, UNITS 1 AND 2; AND THREE MILE ISLAND NUCLEAR STATION, UNIT 1 - REQUEST FOR ADDITIONAL INFORMATION REGARDING APPROVAL OF CYBER SECURITY PLAN (TAC NOS. ME4298, ME4299, ME4301, ME4302, ME4303, ME4304, ME4305, ME4306, ME4307, ME4308, ME4309, ME 4310, ME4311, ME4312, ME4313, AND ME4314)

Dear Mr. Pacilio:

By letter to the Nuclear Regulatory Commission (NRC, the Commission) dated July 23, 2010 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML102070168 (non-public)), Exelon Generation Company, LLC submitted its Cyber Security Plan (CSP) as supplemented by letters dated September 24, November 18, and December 21, 2010, (ADAMS Accession Nos. ML102670438, ML103230042, and ML103550541, respectively). The July 23, 2010, submittal superseded in its entirety the CSP dated November 23, 2009.

The July 23, 2010, CSP is based on the Nuclear Energy Institute (NEI) 08-09, Revision 6, which the NRC staff stated, in its letter dated May 5, 2010 (ADAMS Accession No. ML101190371), would be acceptable for use by licensees to comply with the requirements of Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54 with the exception of the definition of "cyber attack."

The NRC staff is reviewing your submittal and has determined that additional information is required to complete the review. The specific information requested is addressed in the enclosure to this letter. During a discussion with Mr. Douglas Walker of your staff on February 24, 2011, it was agreed that you would provide a response 30 days from the date of this letter. It should be noted that the response to request for additional information No. 2 (RAI 2) will be used to support a license condition at each facility concerning the revised CSP implementation schedule containing the key milestone dates as discussed in 10 CFR 73.54.

The NRC staff considers that timely responses to requests for additional information help ensure sufficient time is available for NRC staff review and contribute toward the NRC's goal of

M. Pacilio

- 2 -

efficient and effective use of NRC staff resources. If circumstances result in the need to revise the requested response date, please contact me before the response date at (301) 415-2315.

Sincerely,

/RA/

Eva A. Brown, Senior Project Manager
Plant Licensing Branch III-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. STN 50-456, 50-457, 50-454,
50-455, 50-461, 50-237, 50-249, 50-373,
50-374, 50-352, 50-353, 50-219, 50-277,
50-278, 50-254, 50-265, and 50-289

Enclosure:
Request for Additional Information

cc w/encl: Distribution via Listserv

REQUEST FOR ADDITIONAL INFORMATION

RELATED TO CYBER SECURITY PLAN REQUEST

FOR BRAIDWOOD STATION, UNIT 1 AND 2; BYRON STATION, UNIT NOS. 1 AND 2;
CLINTON POWER STATION, UNIT NO. 1; DRESDEN NUCLEAR POWER STATION, UNITS 2
AND 3; LASALLE COUNTY STATION, UNITS 1 AND 2; LIMERICK GENERATING STATION,
UNITS 1 AND 2; OYSTER CREEK NUCLEAR GENERATING STATION; PEACH BOTTOM
ATOMIC POWER STATION, UNITS 2, AND 3; QUAD CITIES NUCLEAR POWER STATION,
UNITS 1 AND 2; AND THREE MILE ISLAND NUCLEAR STATION, UNIT 1
DOCKET NOS. STN 50-456, STN 50-457, STN 50-454, STN 50-455, 50-461, 50-237, 50-249,
50-373, 50-374, 50-352, 50-353, 50-219, 50-277, 50-278, 50-254, 50-265, AND 50-289

Records Retention

Title 10 of the *Code of Federal Regulations* (10 CFR) Paragraph 73.54(c)(2) requires licensees to design a cyber security program to ensure the capability to detect, respond to, and recover from cyber attacks. Furthermore, 10 CFR 73.54(e)(2)(i) requires licensees to maintain a cyber security plan (CSP) that describes how the licensee will maintain the capability for timely detection and response to cyber attacks. The ability for a licensee to detect and respond to cyber attacks requires accurate and complete records and is further supported by 10 CFR 73.54(h), which states that the licensee shall retain all records and supporting technical documentation required to satisfy the requirements of 10 CFR 73.54 as a record until the Nuclear Regulatory Commission (NRC, the Commission) terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the NRC.

Section 4.13 of the licensee's Cyber Security Plan (CSP) states that Critical Digital Asset (CDA) audit records and audit data (e.g., operating system logs, network device logs) are retained for a period of time that is less than what is required by 10 CFR 73.54(h).

RAI-1: Explain the deviation from the 10 CFR 73.54(h) requirement to retain records and supporting technical documentation until the Commission terminates the license (or to maintain superseded portions of these records for at least 3 years) and how that meets the requirements of 10 CFR 73.54.

ENCLOSURE

Implementation Schedule

The regulation at 10 CFR 73.54, "Protection of digital computer and communication systems and networks," requires licensees to submit a CSP that satisfies the requirements of this section for the Commission review and approval. Furthermore, each submittal must include a proposed implementation schedule and the implementation of the licensee's cyber security program must be consistent with the approved schedule. Paragraph 73.54(a) of 10 CFR requires licensees to 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.

The completion of several key intermediate milestones listed below would demonstrate progress toward meeting the requirements of 10 CFR 73.54. The NRC staff's expectation is that the key intermediate milestones will be completed in a timely manner, but no later than December 31, 2012. The key CSP implementation milestones are as follows:

- Establish, train and qualify Cyber Security Assessment Team, as described in Section 3.1.2, "Cyber Security Assessment Team," of the CSP.
- Identify Critical Systems and CDAs, as described in Section 3.1.3, "Identification of Critical Digital Assets," of the CSP.
- Implement cyber security defense-in-depth architecture by installation of [deterministic one-way] devices, as described in Section 4.3, "Defense-In-Depth Protective Strategies" of the CSP.
- Implement the management, operational and technical cyber security controls that address attacks promulgated by use of portable media, portable devices, and portable equipment as described in Appendix D Section 1.19 "Access Control for Portable and Mobile Devices," of Nuclear Energy Institute (NEI) 08-09, Revision 6.
- Implement observation and identification of obvious cyber-related tampering to existing insider mitigation rounds as described in Appendix E, Section 4.3, "Personnel Performing Maintenance and Testing Activities," and Appendix E, Section 10.3, "Baseline Configuration" of NEI 08-09, Revision 6.
- Identify, document, and implement cyber security controls to physical security target set CDAs in accordance with Section 3.1.6, "Mitigation of Vulnerabilities and Application of Cyber Security Controls," of the CSP.
- Ongoing monitoring and assessment activities will commence for those target set CDAs whose security controls have been implemented, as described in Section 4.4, "Ongoing Monitoring and Assessment," of the CSP

- Full implementation of the CSP for all safety, security, and emergency preparedness functions.

RAI 2: Provide a revised CSP implementation schedule that identifies the appropriate tones, completion dates, supporting rationale, and level of detail to allow the NRC to evaluate the licensee's proposed schedule and associated milestone dates which include the final completion date. It is the NRC's intention to develop a license condition incorporating the revised CSP implementation schedule containing the key milestone dates.

Scope of Systems

Paragraph 73.54(a) of 10 CFR requires licensees to 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 10 CFR 73.1. In addition, 10 CFR 73.54(a)(1) states that the licensee shall protect digital computer and communication systems and networks associated with:

- Safety-related and important-to-safety functions;
- Security functions;
- Emergency preparedness functions, including offsite communications; and
- Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

Subsequent to the issuance of the Cyber Security Rule, the NRC stated that 10 CFR 73.54 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 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML103490344), dated November 19, 2010). The SSCs in the BOP are those that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient and are therefore, within the scope of important-to-safety functions described in 10 CFR 73.54(a)(1). Furthermore, the NRC issued a letter to NEI dated January 5, 2011 (ADAMS Accession No. ML103550480), that provided licensees with additional guidance on one acceptable approach to comply with the Commission's policy determination.

RAI-3: Explain how the scoping of systems provided by Exelon's CSP meets the requirements of 10 CFR 73.54 and the additional guidance provided by the NRC.

M. Pacilio

- 2 -

efficient and effective use of NRC staff resources. If circumstances result in the need to revise the requested response date, please contact me before the response date at (301) 415-2315.

Sincerely,

/RA/

Eva A. Brown, Senior Project Manager
Plant Licensing Branch III-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. STN 50-456, 50-457, 50-454,
50-455, 50-461, 50-237, 50-249, 50-373,
50-374, 50-352, 50-353, 50-219, 50-277,
50-278, 50-254, 50-265, and 50-289

Enclosure:
Request for Additional Information

cc w/encl: Distribution via Listserv

DISTRIBUTION:

PUBLIC

RidsRgn3MailCenter Resource
RidsOgcRp Resource
RidsNrrPMByron Resource
RidsNrrPMClinton Resource
RidsNrrPMDresden Resource
RidsNrrPMJHughey Resource
RidsNrrPMPBamford Resource
RidsNrrLASRohrer Resource
RidsNrrLAABaxter Resource

LPL3-2 R/F LPL1-2 R/F
RidsNrrDorLp3-2 Resource
RidsNrrPMBraidwood Resource
RidsNrrDorLp1-2 Resource
RidsNrrLaSalle Resource
RidsNrrPMQuadCities Resource
RidsAcrsAcnw&mMailCenter Resource
RidsNrrPMEMiller Resource
RidsNrrDorIDpr Resource
RidsRgn1MailCenter Resource

ADAMS Accession No. ML110550875

OFFICE	LPL3-2/PM	LPL3-2/LA	LPL1-2/BC	LPL3-2/PM
NAME	EBrown	SRohrer	HChernoff	RCarlson (NDiFrancesco for)
DATE	03/02/11	03/02/11	03/04/11	03/04/11

OFFICIAL RECORD COPY