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

March 7, 2011

Mr. Christopher R. Costanzo
Vice President
Duane Arnold Energy Center
3277 DAEC Road
Palo, IA 52324-9785

SUBJECT: DUANE ARNOLD ENERGY CENTER - REQUEST FOR ADDITIONAL INFORMATION RELATED TO LICENSE AMENDMENT REQUEST FOR APPROVAL OF CYBER SECURITY PLAN (TAC NO. ME4287)

Dear Mr. Costanzo:

By letter to the U.S. Nuclear Regulatory Commission (NRC) dated July 14, 2010 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML101960125), as supplemented by letters dated September 27, 2010 (ADAMS Accession No. ML102700605), and November 17, 2010 (ADAMS Accession No. ML103220283), NextEra Energy Duane Arnold, LLC (the licensee) submitted a request for approval of the NextEra Energy Duane Arnold Cyber Security Plan.

The NRC staff is reviewing your submittal and has determined that additional information is required to complete the review. By email dated February 24, 2011, the draft Request for Additional Information (RAI) items were sent to Doreen Barta, a member of your staff. Subsequent to that transmittal we are confirming that those RAI items (see Enclosure) are the final version to which to respond and that the requested date for the response is 30 days after the date of this letter (or the first workday thereafter, if the date falls on a weekend). Further, it was agreed that you would include the full text of each RAI item with your response as a record of these RAI items.

The enclosed RAI items were reviewed in accordance with the guidance provided in 10 CFR Section 2.390. The NRC staff has determined that no security related or proprietary information is contained therein.

The NRC staff considers that timely responses to requests for additional information help ensure that sufficient time is available for staff review and contribute toward the NRC's goal of efficient and effective use of staff resources. If circumstances result in the need to revise the requested response date, please contact me at (301) 415-3079.

Sincerely,

Karl D Feintuch

Karl D. Feintuch, Project Manager
Plant Licensing Branch III-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-331

cc: Distribution via ListServ

REQUEST FOR ADDITIONAL INFORMATION (RAI)

REGARDING APPROVAL OF THE CYBER SECURITY PLAN

DUANE ARNOLD ENERGY CENTER

DOCKET NO. 50-331

RAI 1: 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 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 Section 73.54 as a record until 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 Commission.

The licensee's Cyber Security Plan (CSP) in Section 4.13 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).

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.

RAI 2: 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 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 (Items (a) through (g) below) would demonstrate progress toward meeting the requirements of 10 CFR 73.54. The Nuclear Regulatory Commission (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:

(a) Establish, train and qualify Cyber Security Assessment Team, as described in Section 3.1.2, "Cyber Security Assessment Team," of the CSP

(b) Identify Critical Systems and CDAs, as described in Section 3.1.3, "Identification of Critical Digital Assets," of the CSP.

(c) 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.

(d) 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.

(e) 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.

(f) 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.

(g) 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.

(h) Full implementation of the CSP for all safety, security, and emergency preparedness functions.

Provide a revised CSP implementation schedule that identifies the appropriate milestones, 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 your revised CSP implementation schedule containing the key milestone dates.

RAI 3: 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:

(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.

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.

Explain how the scoping of systems provided by licensee's CSP meets the requirements of 10 CFR 73.54 and the additional guidance provided by the NRC.

The NRC staff considers that timely responses to requests for additional information help ensure that sufficient time is available for staff review and contribute toward the NRC's goal of efficient and effective use of staff resources. If circumstances result in the need to revise the requested response date, please contact me at (301) 415-3079.

Sincerely,

/RA/

Karl D. Feintuch, Project Manager
Plant Licensing Branch III-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-331

Enclosure: As stated

cc w/encl: Distribution via ListServ

DISTRIBUTION:

PUBLIC LPL3-1 R/F	RidsNrrDorlDpr Resource	PPederson, NSIR
RidsNrrDorlLpl3-1 Resource	RidsAcrsAcnw_MailCTR Resource	
RidsNRRPMDuaneArnold Resource	RidsOgcRp Resource	
RidsNrrLABTully Resource	RidsRgn3MailCenter Resource	

ADAMS Accession Number: ML110620630 *via memo dated 2/18/11

OFFICE	LPL3-1/PM	LPL3-1/LA	NSIR/DSP/ISCPB/BC	LPL3-1/BC
NAME	KFeintuch	BTully	CErlanger*	RPascarelli
DATE	03/07/11	03/04/11	02/18/11	03/07/11

OFFICIAL RECORD COPY