Omaha Public Power District
444 South 16th Street Mall
Omaha, NE 68102-2247

March 31, 2011
LIC-11-0033

U.S. Nuclear Regulatory Commission
Attn: Document Control Desk
Washington, D.C. 20555

References:
1. Docket No. 50-285
2. Letter from OPPD (J. A. Reinhart) to NRC (Document Control Desk), "Fort Calhoun Station, Unit No.1, License Amendment Request (LAR), Request for Approval of the FCS/OPPD Cyber Security Plan," dated July 26, 2010 (LIC-10-0055) (ML 102080452) (TAC No. ME4380)
3. Letter from OPPD (J. A. Reinhart) to NRC (Document Control Desk), "Fort Calhoun Station (FCS), Unit No.1, Supplement to FCS / OPPD Cyber Security Plan License Amendment Request (LAR) Regarding Balance of Plant Systems within the Scope of the Program," dated November 30, 2010 (LIC-10-0101) (ML 102080452) (TAC No. ME4380)
4. Letter from NRC (L. E. Wilkins) to OPPD (D. J. Bannister), "Fort Calhoun Station, Unit No. 1 – Request for Additional Information Regarding Revision to the Renewed Facility Operating License and Request for Review and Approval of the Cyber Security Plan (TAC No. ME4380)," dated March 2, 2011 (NRC-11-0027)

SUBJECT: Response to NRC Generic Request for Additional Information (RAI)

In Reference 2, the Fort Calhoun Station (FCS), Unit No. 1 / Omaha Public Power District (OPPD) Cyber Security Plan (i.e., the Plan) was submitted for NRC review and approval. In Reference 3, OPPD revised the Plan to clarify that certain structures, systems, and components (SSCs) in the balance of plant (BOP) will be protected by the Plan. In Reference 4, the NRC requested additional information concerning the Plan and OPPD's response is attached.

Please note that the FCS Plant Review Committee (PRC) must approve the Plan and Implementation Schedule changes described in the attachments. Therefore, OPPD commits to revise and resubmit the Plan within 15 days of this response (AR 46159).

If you have any questions regarding this submittal, please contact Mr. Bill Hansher at (402) 533-6894.

Sincerely,

J. B. Herman
Division Manager-Nuclear Engineering

JBH/CJS/mle

Attachments: 1. OPPD Response to Generic Request for Additional Information (RAI)
2. Cyber Security Plan Implementation Schedule

c: E. E. Collins, Jr., NRC Regional Administrator, Region IV
L. E. Wilkins, NRC Project Manager
J. C. Kirkland, NRC Senior Resident Inspector

OPPD Response to NRC Request for Additional Information

Generic Request for Additional Information (RAI)

NRC 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.

OPPD Response

Section 4.13, *Document Control And Records Retention And Handling* of the FCS / OPPD Cyber Security Plan will be revised to incorporate the following text:

"FCS / OPPD has established the necessary measures and governing procedures to ensure that sufficient records of items and activities affecting cyber security are developed, reviewed, approved, issued, used, and revised to reflect completed work.

The following are examples of records or supporting technical documentation that are retained as a record until the Commission terminates the license for which the records are developed. Superseded portions of these records are retained for three years unless otherwise specified by the Commission in accordance with the requirements of 10 CFR 73.54(h):

- Modification records for CDAs;
- Analyses, basis, conclusions, and determinations used to establish a component as a CDA;

- Cyber Security Plan;
- Written Policies and Procedures that implement and maintain the Cyber Security program, with records of changes;
- Corrective Action records related to Cyber Security non-conformance or adverse conditions;
- Documentation of periodic Cyber Security Program reviews and Program audits;
- Vulnerability notifications determined to adversely impact CDAs and the associated analyses, assessments and dispositions;
- Training records to document personnel qualifications and program implementation and maintenance; and
- Audit records, which are electronic or manual event records (logs) that facilitate the identification and analysis of cyber security attacks and are developed in accordance with Appendix D, Section 2, *Audit and Accountability.*
    - The scope of auditable events is developed in accordance with Appendix D, Section 2.2, *Auditable Events.* Events identified for auditing are recorded in accordance with Appendix D, Section 2.3, *Content of Auditable Records* and Appendix D, Section 2.4, *Audit Storage Capacity* (for electronic audit records). The source of auditable events (electronic and non-electronic) include, but are not limited to:
        - Operating system logs
        - Service and application logs
        - Network device logs
        - Access Logs
    - Audit records of auditable events are retained to document access history, as well as to discover the source of cyber attacks or other security-related incidents affecting CDAs or SSEP functions, or both. These records are reviewed and analyzed in accordance with the policies, procedures, and programs implementing Appendix D, Section 2.6, *Audit Review, Analysis and Reporting.* The review and analysis is conducted consistent with maintaining 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. Superseded records (or portions thereof) are then retained for three years, after the record has been reviewed and analyzed."

NRC 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.

OPPD Response

Attachment 2 contains a revised CSP implementation schedule that identifies the appropriate milestones, completion dates, and supporting rationale.

NRC 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 [site/licensee]'s CSP meets the requirements of 10 CFR 73.54 and the additional guidance provided by the NRC.

OPPD Response

In Reference 3, OPPD revised its initial license amendment request (Reference 2) to note that the scoping provisions of 10 CFR 73.54 encompass certain structures, systems, and components (SSCs) in the balance of plant (BOP). Reference 3 noted that among the systems to be protected were those SSCs in the BOP out to the first inter-tie with the offsite distribution system whose compromise could result in a reactor scram or transient.

Nevertheless, OPPD will revise the FCS / OPPD Cyber Security Plan to be consistent with the latest NRC guidance on this issue (Adams Accession No. ML103550480). Thus, the following paragraph will replace the paragraph previously added to the FCS / OPPD Cyber Security Plan in Reference 3:

"Within the scope of NRC's cyber security rule at Title 10 of the Code of Federal Regulations (10 CFR) 73.54, systems or equipment that perform important to safety functions include structures, systems, and components (SSCs) in the balance of plant (BOP) that could directly or indirectly affect reactivity at a nuclear power plant and could result in an unplanned reactor shutdown or transient. Additionally, these SSCs are under the licensee's control and include electrical distribution equipment out to the first inter-tie with the offsite distribution system."

FCS / OPPD Cyber Security Plan Implementation Schedule

FCS / OPPD Cyber Security Plan Implementation Schedule

Full implementation of the cyber security program involves many supporting tasks. Major activities include: program and procedure development; performing of individual critical digital asset (CDA) assessments; and identification, scheduling, and implementing individual asset security control design remediation actions through the site configuration management program. These design modifications may be performed on-line or could require a refueling outage for installation.

The extensive workload associated with full implementation of the Cyber Security Plan (CSP) requires prioritization to assure those activities that provide higher degrees of protection against radiological sabotage are performed first. Therefore, the CSP implementation schedule will be implemented with two major milestone dates. The first milestone date of no later than December 31, 2012, includes the activities listed in the table below. The second milestone date, December 31, 2015, includes the completion of all remaining actions that result in the full implementation of the cyber security plan for all applicable Safety, Security, and Emergency Preparedness (SSEP) functions. This date also bounds the completion of all individual asset security control design remediation actions.

Cyber security controls are not applied if the control adversely impacts safety and important to safety, security or emergency preparedness functions.

#	Implementation Milestone	Completion Date	Basis
1	Establish Cyber Security Assessment Team (CSAT) as described in Section 3.1.2 "Cyber Security Assessment Team" of the Cyber Security Plan (CSP).	No later than December 31, 2012	The CSAT, collectively, will need to have digital plant systems knowledge as well as nuclear power plant operations, engineering and nuclear safety experience and technical expertise. The personnel selected for this team may require additional training in these areas help to ensure adequate capabilities to perform cyber security assessments as well as others duties.
2	Identify Critical Systems (CSs) and Critical Digital Assets (CDAs) as described in Section 3.1.3 "Identification of Critical Digital Assets" of the CSP.	No later than December 31, 2012	The scope of 10 CFR 73.54 includes 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. The scope of 10 CFR 73.54 includes structures, systems, and components (SSCs) that have a nexus to radiological health and safety and therefore can directly or indirectly affect reactivity of a nuclear power plant and could

#	Implementation Milestone	Completion Date	Basis
			result in an unplanned reactor shutdown or transient.
3	Implement Installation of a deterministic one-way device between lower level devices (level 0 1,2) and the higher level devices (level 3,4) as described in Section 4.3, "Defense-In-Depth Protective Strategies" of the CSP. Lower security level devices (level 0, 1, 2 devices) that bypass the deterministic device and connect to level 3 or 4 will be modified to prevent the digital connectivity to the higher level or will be modified to meet cyber security requirements commensurate with the level 3 or 4 devices to which they connect. The design modifications that are not finished by the completion date will be documented in the site configuration management and/or change control program to assure completion of the design modification as soon as possible, but no later than the final implementation date.	No later than December 31, 2012	The implementation of communication barriers protects the most critical SSEP functions from remote attacks on plant systems. Isolating the plant systems from the internet as well as from the corporate business systems is an important milestone in defending against external threats. While the deployment of the barriers is critical to protection from external cyber threats, it also prevents remote access to core monitoring and plant data systems for reactor engineers, plant operations, and other plant staff. This elimination of remote access to reactor core monitoring systems may require the development and execution of a detailed change management plan to ensure continued safe operation of the plants. Vendors may be required to develop software revisions to support the model. The modification will be developed, prioritized and scheduled.
4	The security control "Access Control For Portable And Mobile Devices" described in Appendix D 1.19 of NEI 08-09, Revision 6, will be implemented.	No later than December 31, 2012	Portable media devices are used to transfer electronic information (e.g., data, software, firmware, virus engine updates and configuration information) to and from plant process equipment. Careful use of this class of media is required to minimize the spread of malicious software to plant process equipment. The effective implementation of this control may require the coordinated implementation of other complimentary controls to

#	Implementation Milestone	Completion Date	Basis
			ensure adequate mitigation.
5	Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds by incorporating the appropriate elements in Appendix E Section 4.3 "Personnel Performing Maintenance And Testing Activities."	No later than December 31, 2012	Insider mitigation rounds by trained staff look for obvious signs of cyber related tampering and would provide mitigation of observable cyber related insider actions. Implementing steps to add signs of cyber security-related tampering to insider mitigation rounds will be performed by the completion date.
6	Identify, document, and implement NEI 08-09, Rev 6 Appendix D technical cyber security controls in accordance with the Cyber Security Plan Section 3.1.6 "Mitigation of Vulnerabilities and Application of Cyber Security Controls" for CDAs that could adversely impact the design function of physical security target set equipment. The implementation of controls that require a design modification that are not finished by the completion date will be documented in the site configuration management and/or change control program to assure completion of the design modification as soon as possible, but no later than the final implementation date.	No later than December 31, 2012	The site physical protection program provides high assurance that these elements are protected from physical harm by an adversary. The cyber security program will enhance the defense-in-depth nature of the protection of CDAs associated with target sets. Implementing Cyber Security Plan technical controls to target set CDAs provides a high degree of protection against cyber related attacks that could lead to radiological sabotage. Security controls will be addressed in accordance with Cyber Security Plan Section 3.1.6 with the exception of those that require a design modification. Note that the Operational and Management controls, as provided in NEI 08-09, Rev 6, Appendix E, will be implemented in conjunction with the full implementation of the Cyber Security Program. These controls are primarily procedure based programs and must be implemented in coordination with the comprehensive Cyber Security Program. However, a high degree of protection against cyber related attacks is maintained as many of these programs (e.g., physical protection, maintenance and work management, configuration management, operational experience, etc) are currently in place and are well established within the nuclear industry. For the CDAs in scope, Operational and

#	Implementation Milestone	Completion Date	Basis
			Management Security Controls will be addressed under an interim auditable process since not all elements of the Operational and Management (O&M) Security Controls Program as required by NEI 08-09, Rev. 6 will be fully developed and implemented by 12/31/2012.
7	Ongoing monitoring and assessment activities commence, as described in Section 4.4, "Ongoing Monitoring and Assessment" of the CSP, for those target set CDAs whose security controls have been implemented.	No later than December 31, 2012	The ongoing monitoring and assessment activities as described in Section 4.4, "Ongoing Monitoring and Assessment" of the Cyber Security Plan will be implemented for the controls applied to target set CDAs. This action results in the commencement of the cyber security program for target set related CDAs.
8	Full implementation of FCS / OPPD Cyber Security Plan for all SSEP functions will be achieved.	December 31, 2015	By the completion date, FCS / OPPD Cyber Security Plan will be fully implemented for all SSEP functions in accordance with 10 CFR 73.54. This date also bounds the completion of all individual asset security control design remediation actions including those that require a refuel outage for implementation.