Mary G. Korsnick
Chief Nuclear Officer,
SVP-Chief Operations Officer

Constellation Energy Nuclear Group, LLC
100 Constellation Way, Suite 200C
Baltimore, MD 21202
Office 410-470-5133
Fax 443-213-6739
Maria.Korsnick@cengllc.com

CENG
a joint venture of
Constellation Energy EDF

April 4, 2011

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

ATTENTION: Document Control Desk

SUBJECT: **Calvert Cliffs Nuclear Power Plant**
Unit Nos. 1 & 2; Docket Nos. 50-317 & 50-318
Nine Mile Point Nuclear Station
Unit Nos. 1 & 2; Docket Nos. 50-220 & 50-410
R. E. Ginna Nuclear Power Plant
Docket No. 50-244

Response to Request for Additional Information: Cyber Security Plan

REFERENCES:
(a) Letter from D. V. Pickett (NRC) to M. G. Korsnick (CENG), dated March 3, 2011, Request for Additional Information Re: Cyber Security Plan-Calvert Cliffs Nuclear Power Plant, Unit Nos. 1 and 2, R.E. Ginna Nuclear Power Plant, Nine Mile Point Nuclear Station, Unit Nos. 1 and 2 – (TAC Nos. ME4328, ME4329, ME4330, ME4331, and ME4332)

(b) Letter from M. G. Korsnick (CENG) to Document Control Desk (NRC), dated September 27, 2010, Notification Letter Designating Balance of Plant Systems within the Cyber Security Rule Scope

Reference (a) requested additional information regarding the Constellation Energy Nuclear Group (CENG) Cyber Security Plan. The responses are in Attachment (1).

In Reference (b), we committed to revising our Cyber Security Plan to clarify the scope of systems that will be protected under the provisions of the Plan. Since Request for Additional Information (RAI) 3 in Reference (a) asks for the same information, the response to RAI 3 satisfies that commitment.

It is our understanding that the Nuclear Regulatory Commission (NRC) and the Nuclear Energy Institute have met several times to discuss template language providing the information the NRC requested in Reference (a). The responses to the RAIs in Attachment (1) to this letter follow the Nuclear Energy Institute template language.

S001A
NRR

The changes to the Cyber Security Plan discussed in Attachment (1) will require a revision to the Plan, which will be submitted no later than July 1, 2011, pending NRC concurrence with the RAI responses.

Regulatory commitments in this correspondence are detailed in Attachment (2).

Should you have any questions concerning this letter, or require additional information, please contact Bruce Montgomery at 410-470-3777 or Bruce.Montgomery@cengllc.com.

Sincerely,

Mary G. Korsnick

MGK/EMT/bjd

Attachment: (1) Response to Request for Additional Information
(2) Regulatory Commitments

cc: D. V. Pickett, NRC
R. V. Guzman, NRC
W. M. Dean, NRC
J. T. Wiggins, NRC
E. J. Leeds, NRC
M. Moon, NERC
Resident Inspector, NRC (Calvert Cliffs)
Resident Inspector, NRC (Ginna)
Resident Inspector, NRC (Nine Mile Point)
S. Gray, Maryland DNR

ATTACHMENT (1)

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Constellation Energy Nuclear Group, LLC
April 4, 2011

ATTACHMENT (1)

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

RAI 1 Records Retention

Title 10 of the Code of Federal Regulations (10 CFR) Section 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 Commission terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least three years after the record is superseded, unless otherwise specified by the Commission.

The licensee's 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 three years) and how that meets the requirements of 10 CFR 73.54.

Response:

The Constellation Energy Nuclear Group (CENG) CSP will be revised as follows:

4.13 Document Control And Records Retention And Handling

Constellation Energy Nuclear Group 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;
- CSP;
- 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 NEI 08-09, Revision 6, 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 Events" and Appendix D, Section 2.4, "Audit Storage Capacity (for electronic audit records)." The sources 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 Safety, Security, and Emergency Preparedness (SSEP) functions, or both. These records are reviewed and analyzed in accordance with 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 retained for three years, after the record has been reviewed and analyzed.

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. Title 10 CFR 73.54(a) 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 (h) 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 (CSAT), 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.

Response:

Regarding the license condition, it is our position that it is not necessary to include the implementation schedule. This submittal of the schedule constitutes a regulatory commitment on the part of the three licensees that make up the CENG fleet. We have a procedure that governs the control of regulatory commitments. Detailing an implementation schedule in the license does not add to the obligation to comply with the schedule.

We note that item (h) for full implementation is not included in the actions to be accomplished by December 31, 2012, as agreed by NEI and NRC. Full implementation in the schedule presented here will be accomplished by February 26, 2016.

The following text and schedule supersede the text and schedule previously submitted by Constellation Energy Nuclear Group, LLC letter dated July 16, 2010.

Full implementation of the cyber security program involves many supporting tasks. Major activities include: program and procedure development; performance of individual CDA assessments; and identifying, 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 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 December 31, 2012, includes activities that CENG will accomplish that, once implemented; provide a high degree of protection against cyber-related attacks that could lead to radiological sabotage. The second milestone date, February 26, 2016 includes the completion of all remaining actions that result in the full implementation of the CSP for all applicable 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.

Task #	Implementation Milestone	Completion Date	Basis
1	Establish a CSAT as described in Section 3.1.2, "Cyber Security Assessment Team," of the 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 to ensure adequate capabilities to perform cyber security assessments, as well as others duties.
2	Identify Critical Systems and 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 result in an unplanned reactor shutdown or transient.

ATTACHMENT (1)

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Task #	Implementation Milestone	Completion Date	Basis
3	Implement installation of a deterministic one-way device between lower level devices (levels 0, 1, 2) and the higher level devices (levels 3, 4) as described in Section 4.3, "Defense-In-Depth Protective Strategies," of the CSP. Lower security level devices (levels 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	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, Section 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 ensure adequate mitigation.
5	Implement observation and identification of obvious cyber-related tampering to existing insider mitigation rounds by incorporating the appropriate elements in NEI 08-09, Revision 6, Appendix E, Section 4.3, "Personnel Performing Maintenance and Testing Activities."	No later than: December 31, 2012	Insider mitigation rounds by trained staff that are looking for obvious signs of cyber related tampering 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.

Task #	Implementation Milestone	Completion Date	Basis
6	Identify, document, and address cyber security controls in accordance with CSP 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 CSP security 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 CSP Section 3.1.6, with the exception of those that require a design modification. The implementation of controls requiring 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.
7	Ongoing monitoring and assessment activities commence, as described in CSP Section 4.4, "Ongoing Monitoring and Assessment," 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 CSP Section 4.4, "Ongoing Monitoring and Assessment," 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 CENG Fleet CSP for all SSEP functions will be achieved.	No later than: February 26, 2016	By the completion date, the CENG Fleet CSP 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 refueling outage for implementation.

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

Response:

The CENG Cyber Security Plan, Section 2.1, "Scope and Purpose," currently contains language that mimics 10 CFR 73.54(a). We consider this sufficient to show that the scope of the Plan meets the requirements of the rule. Additionally, Section 2.1 will be revised to include in the scope of the plan the SSCs in the BOP that could directly or indirectly affect reactivity at a nuclear power plant and could result in an unplanned reactor shutdown or transient.

ATTACHMENT (2)

REGULATORY COMMITMENTS

Constellation Energy Nuclear Group, LLC
April 4, 2011

ATTACHMENT (2)

REGULATORY COMMITMENTS

The following table identifies the regulatory commitments in this document. Any other statements in this submittal represent intended or planned actions. They are provided for information purposes and are not considered to be regulatory commitments.

COMMITMENT	SCHEDULED COMPLETION DATE
Revise Section 4.13 of the Cyber Security Plan (RAI 1)	7/1/2011
Complete Tasks 1- 7 in the implementation schedule (RAI 2)	12/31/2012
Complete Task 8 in the implementation schedule is completed (RAI 2)	2/26/2016
Revise Section 2.1 of the Cyber Security Plan (RAI 3)	7/1/2011