NEI 08-09 will be revised as follows:

4.13 Document Control And Records Retention And Handling

[Site/Licensee] 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that are retained as a record until the Commission terminates the license for which the records are developed., Superseded portions of these records are retained for three years unless otherwise specified by the Commission in accordance with the requirements of 10 CFR 73.54(h):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 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 Audible Events* 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 accordance with [policies, procedures, 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.