U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Public Meeting

Records Retention Requirements to Support Cyber Security

December 16, 2010

Overview

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- **Regulatory requirement for records retention**
- **Regulatory Guide 5.71 view of records retention**

Regulatory Requirement

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- 10 CFR 73.54(h) The licensee shall retain all records and supporting technical documentation required to satisfy the requirements of this section as a record until the Commission terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified by the Commission.
- What should be considered:
  - records and supporting technical documentation
- Requirement:
  - required to satisfy the requirements of this section (73.54)
- Duration:
  - until the Commission terminates the license

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

C.5 Records Retention and Handling

In accordance with 10 CFR 73.54(h), the licensee must retain all records and supporting technical documentation required to satisfy the requirements of this regulation until the Commission terminates the license for which the records were developed. Furthermore, the licensee must maintain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the Commission.

An acceptable method for complying with this requirement is for the licensee to maintain records or supporting technical documentation so that inspectors, auditors, or assessors will have the ability to evaluate incidents, events, and other activities that are related to any of the cyber security elements described, referenced, and contained within the licensee's NRC-approved cyber security plan. Records required for retention include, but are not limited to, digital records, log files, audit files, and nondigital records that capture, record, and analyze network and CDA events. Licensees should retain these records to document access history and discover the source of cyber attacks or other security-related incidents affecting CDAs or SSEP functions. Section 5 of Appendix A to this guide includes a template for the licensee to use in preparing the cyber security plan regarding records retention and handling of security controls.

Regulatory Guide 5.71

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

APPENDIX A - GENERIC CYBER SECURITY PLAN TEMPLATE

A.5 DOCUMENT CONTROL AND RECORDS RETENTION AND HANDLING

[Licensee/Applicant] 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. [Licensee/Applicant] will retain records and supporting technical documentation required to satisfy the requirements of 10 CFR 73.54 and 10 CFR 73.55, Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage," until the NRC terminates the facility operating license. Records required for retention include, but are not limited to, all digital records, log files, audit files, and nondigital records that capture, record, and analyze network and CDA events. These records are retained to document access history and discover the source of cyber attacks or other security-related incidents affecting CDAs or SSEP functions or both. [Licensee/Applicant] will retain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the NRC.