NUCLEAR ENERGY INSTITUTE

DRAFT Cyber Security Records White Paper

Cyber Security Task Force

Bill Gross

12/13/2010

The objective of this paper is to establish what cyber security records are to be kept by each licensee as required by 73.54 (h). Also this paper addresses what records listed in RG 5.71 and NEI 08-09 are not required to be retained by the cyber security regulation.

Cyber Security Records White Paper

Contents

Cyber Security Records White Paper

1.1 OBJECTIVE

The objective of this paper is to establish and identify cyber security "Records" to be maintained by each license as required by 73.54 (h). Also this paper addresses those electronic data records listed in RG 5.71 and NEI 08-09 that are not required to be retained by the cyber security regulation. Security regulation including 10CFR73.70 and 10CFR73.54 are used as references to support the basis for this determination.

The approach used is:

1. First, evaluating the cyber security regulations for key words.
2. Next, the requirements of the security regulation is used to develop a logical flow of the cyber security regulations which states "the licensee shall retain all records and supporting technical documentation required to satisfy the **requirements of this section"**
3. Finally, based on the logical flow of the requirements contained in security regulations, a table of all Records and supporting technical documentation required to be maintained was developed.

Based upon the table of all Records and supporting technical documentation required to be maintained, the records retention section of NEI 08-09 and RG 5.71 was evaluated. The security controls which specify "record" requirements described in NEI 08-09 Appendices D and E were evaluated and this document explains how these "records" which are electronic data log files are not NOT required to be maintained by the cyber security regulations.

Finally, recommendations are provided for revising the records retention section of NEI 08-09 and RG 5.71.

1.2 REGULATIONS AND RECORDS

In order to clearly delineate those "Records" required by regulation, as opposed to "records" noted in NEI 08-09 and RG 5.71, the definition of Records in 10CFR73.70 will be utilized.

"Each record required by this part must be legible throughout the retention period specified by each Commission regulation. The record may be the original or a reproduced copy or a microform provided that the copy or microform is authenticated by authorized personnel and that the microform is capable of producing a clear copy throughout the required retention period. The record may also be stored in electronic media with the capability for producing legible, accurate, and complete records during the required retention period. Records such as letters, drawings, specifications, must include all pertinent information such as stamps, initials, and signatures. The licensee shall maintain adequate safeguards against tampering with and loss of records."

10CFR73.54(h) describes cyber security "Records" as: 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.

Technical documentation is defined as those written products that are required to be "developed and maintained" or "established, implemented, and maintained" by 10CFR73.54. This includes procedures, policies, the Cyber Security Plan, and the Cyber Security Program.

The industry calls the Records to be maintain to meet 73.54(h), big "R" Records and those not required to be kept little "r" records.

1.3 CYBER SECURITY REGULATIONS

The following is the cyber security regulations with key words highlighted in **bold**. The key words will be used to determine the logical flow of the regulation and the requirements in the regulations.

(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.

a) Each licensee subject to the **requirements of this section** shall 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 § 73.1.
(1) 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.

(2) The licensee **shall protect** the systems and networks identified in paragraph (a)(1) of this section from cyber attacks that would:

(i) Adversely impact the integrity or confidentiality of data and/or software;
(ii) Deny access to systems, services, and/or data; and
(iii) Adversely impact the operation of systems, networks, and associated equipment.

(b) **To accomplish this**, the licensee shall:

(1) **Analyze** digital computer and communication systems and networks and **identify** those assets that must be protected against cyber attacks to satisfy paragraph (a) of this section,
(2) **Establish, implement, and maintain** a **cyber security program** for the protection of the assets identified in paragraph (b)(1) of this section; and
(3) **Incorporate** the cyber security program as a component of the physical protection program.

(c) The **cyber security program must be designed** to:

(1) **Implement security controls** to protect the assets identified by paragraph (b)(1) of this section from cyber attacks;
(2) **Apply and maintain defense-in-depth protective strategies** to ensure the capability to detect, respond to, and recover from cyber attacks;
(3) **Mitigate** the adverse affects of cyber attacks; and

(4) **Ensure** that the functions of protected assets identified by paragraph (b)(1) of this section are not adversely impacted due to cyber attacks.

(d) As part of the cyber security program, the licensee shall:

(1) **Ensure** that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the **training** necessary to perform their assigned duties and responsibilities.

(2) **Evaluate and manage cyber risks**.

(3) Ensure that **modifications** to assets, identified by paragraph (b)(1) of this section, are evaluated before implementation to ensure that the cyber security performance objectives identified in paragraph (a)(1) of this section are maintained.

(e) The licensee shall **establish, implement, and maintain** a **cyber security plan** that implements the cyber security program requirements of this section.

(1) The cyber security plan must **describe** how the requirements of this section will be implemented and must account for the site-specific conditions that affect implementation.

(2) The cyber security plan **must include measures** for incident response and recovery for cyber attacks. The cyber security **plan must describe** how the licensee will:

(i) **Maintain** the capability for timely detection and response to cyber attacks;

(ii) **Mitigate** the consequences of cyber attacks;

(iii) **Correct** exploited vulnerabilities; and

(iv) **Restore** affected systems, networks, and/or equipment affected by cyber attacks.

(f) The licensee **shall develop and maintain written policies and implementing procedures** to implement the cyber security plan. Policies, implementing procedures, site-specific analysis, and other supporting technical information used by the licensee need not be submitted for Commission review and approval as part of the cyber security plan but are subject to inspection by NRC staff on a periodic basis.

(g) The licensee shall **review the cyber security program** as a component of the physical security program in accordance with the requirements of § 73.55(m), including the periodicity requirements.

1.4 FLOW OF THE REGULATIONS

The flow of the regulations was determined by a logical reading of the regulations. The following is the flow that was found. The regulations are summarized in this section.

The licensee **shall protect** digital computer and communication systems and networks associated with SSEP functions (i.e.; 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 licensee **shall protect** the systems and networks from cyber attacks

To accomplish this, the licensee shall:

Analyze digital computer and communication systems and networks and **identify** those assets that must be protected against cyber attacks to satisfy paragraph (a) of this section,
Establish, implement, and maintain a **cyber security program** for the protection of the assets identified in paragraph (b)(1) of this section; and
Incorporate the cyber security program as a component of the physical protection program.
Establish a security plan that **describes** how the requirements will be implemented and must account for the site-specific conditions that affect implementation and **includes measures** for incident response and recovery for cyber attacks. The cyber security **plan must describe** how the licensee will address certain items.

Maintain the capability for timely detection and response to cyber attacks;
Mitigate the consequences of cyber attacks;
Correct exploited vulnerabilities; and
Restore affected systems, networks, and/or equipment affected by cyber attacks.

As part of the cyber security program, the licensee shall:

Train
Evaluate and manage cyber risks.
Manage modifications to assets
Establish, implement, and maintain a **cyber security plan.**
Develop and maintain written policies and implementing procedures
R**eview the cyber security program**

1.5 RECORDS REQUIREMENT SUMMARIZED

The following is the records requirement summarized based on the flow of the regulations provided above.

[Licensee] shall retain the following records and supporting technical documentation 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:

Records and supporting technical documentation required	**Reference**
Analysis of digital computer and communication systems and networks and **identification** of those assets that must be protected against cyber attacks	(1) **Analyze** digital computer and communication systems and networks and **identify** those assets that must be protected against cyber attacks to satisfy paragraph (a) of this section,
Implementation, and maintenance of the cyber security program	(2) **Establish, implement, and maintain** a **cyber security program** for the protection of the assets identified in paragraph (b)(1) of this section
Incorporation the cyber security program as a component of the physical protection program	(3) **Incorporate** the cyber security program as a component of the physical protection program.

Cyber Security Plan	(2) The cyber security plan **must include measures** for incident response and recovery for cyber attacks. The cyber security **plan must describe** how the licensee will: (i) Maintain the capability for timely detection and response to cyber attacks; (ii) Mitigate the consequences of cyber attacks; (iii) Correct exploited vulnerabilities; and (iv) Restore affected systems, networks, and/or equipment affected by cyber attacks.
Design of the cyber security program to address 1) **Implement security controls** to protect the assets identified by paragraph (b)(1) of this section from cyber attacks; (2) **Apply and maintain defense-in-depth protective strategies** to ensure the capability to detect, respond to, and recover from cyber attacks; (3) **Mitigate** the adverse affects of cyber attacks; and (4) **Ensure** that the functions of protected assets identified by paragraph (b)(1) of this section are not adversely impacted due to cyber attacks	(c) The cyber security program **must be designed** to: (1) **Implement security controls** to protect the assets identified by paragraph (b)(1) of this section from cyber attacks; (2) **Apply and maintain defense-in-depth protective strategies** to ensure the capability to detect, respond to, and recover from cyber attacks; (3) **Mitigate** the adverse affects of cyber attacks; and (4) **Ensure** that the functions of protected assets identified by paragraph (b)(1) of this section are not adversely impacted due to cyber attacks
Training	1) **Ensure** that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the **training** necessary to perform their assigned duties and responsibilities.
Evaluation and management of cyber risks	(2) **Evaluate** and **manage** cyber risks.
Modifications	(3) Ensure that **modifications** to assets, identified by paragraph (b)(1) of this section, are evaluated before implementation to ensure that the cyber security performance objectives identified in paragraph (a)(1) of this section are maintained.
Cyber Security Plan	(e) The licensee shall **establish, implement, and maintain** a **cyber security plan** that implements the cyber security program requirements of this section.
Written policies and implementing procedures.	(f) The licensee **shall develop and maintain written policies and implementing procedures** to implement the cyber security plan. Policies, implementing procedures, site-specific analysis, and other supporting technical information used by the licensee need not be

	submitted for Commission review and approval as part of the cyber security plan but are subject to inspection by NRC staff on a periodic basis.
Review of the cyber security program.	(g) The licensee shall **review the cyber security program** as a component of the physical security program in accordance with the requirements of § 73.55(m), including the periodicity requirements.

1.6 EVALUATION OF THE CYBER SECURITY RECORD REQUIREMENTS IN NEI 08-09 AGAINST THE REQUIREMENTS IN THE CYBER SECURITY RULE

The following is quoted directly from NEI 08-09 Rev 6:

> 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 will be retained 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:
>
> - Records of the assessment described in Section 3.1 of this Plan;
> - Records that are generated in the Establishment, Implementation, and Maintenance of the Cyber Security Program;
> - Records of Addition and Modification of Digital Assets; and
> - Records and supporting technical documentation required to satisfy the requirements of the Rule
>
> CDA audit records will be retained for no less than 12 months. CDA auditing capabilities are configured in accordance with section 3.1.6 of this plan.
>
> Where a central logging server is employed, the audit records received will be retained for no less than 12 months.
>
> The following audit data will be retained:
> - Audit data described in Appendix D, 2.3, "Content of audit records"
> - Audit data that support Appendix E, "Defense-in-Depth" security control will be retained to provide support for after-the-fact investigations of security attacks and satisfy the requirements of 10 CFR 73.54 and 10 CFR 73.55.
>
> Audit (digital and non-digital) data include:
> - Operating system logs
> - Service and application logs
> - Network device logs

For the purposes of this Plan, audit data is not required to be maintained under the QA Records Program.

Individual Cyber Security Training Records will be documented and maintained for 3 years.

The following lists Records and supporting technical documentation in NEI 08-09 Rev 6 required by the cyber security regulations.

The NEI 08-09 Rev 6 requirements in **bold** are specific and those not in bold are not specific. Those that are not specific need to be clarified.

Records and supporting technical documentation required by the cyber security regulations	**NEI 08-09 Rev 6 requirement**
Analysis of digital computer and communication systems and networks and **identification** of those assets that must be protected against cyber attacks	**Records of the assessment described in Section 3.1 of this Plan**
Implementation, and maintenance of the cyber security program	**Records that are generated in the Establishment, Implementation, and Maintenance of the Cyber Security Program**
Incorporation the cyber security program as a component of the physical protection program	Records and supporting technical documentation required to satisfy the requirements of the Rule
Cyber Security Plan	Records and supporting technical documentation required to satisfy the requirements of the Rule
Design of the cyber security program to address specific items	Records and supporting technical documentation required to satisfy the requirements of the Rule
Training	**Individual Cyber Security Training Records will be documented and maintained for 3 years.**
Evaluation and management of cyber risks	Records and supporting technical documentation required to satisfy the requirements of the Rule
Modifications	**Records of Addition and Modification of Digital Assets**
Cyber Security Plan	Records and supporting technical documentation required to satisfy the requirements of the Rule
Written policies and implementing procedures.	Records and supporting technical documentation required to satisfy the requirements of the Rule
Review of the cyber security program.	Records and supporting technical documentation required to satisfy the requirements of the Rule

The following lists records and supporting technical documentation in NEI 08-09 Rev 6 NOT required by the cyber security regulations.

The following audit data will be retained:

- Audit data described in Appendix D, 2.3, "Content of audit records"
- Audit data that support Appendix E, "Defense-in-Depth" security control will be retained to provide support for after-the-fact investigations of security attacks and satisfy the requirements of 10 CFR 73.54 and 10 CFR 73.55.

Audit (digital and non-digital) data include:

- Operating system logs

- Service and application logs
- Network device logs

1.7 EVALUATION OF THE CYBER SECURITY RECORD REQUIREMENTS IN RG 5.71 AGAINST THE REQUIREMENTS IN THE CYBER SECURITY RULE

The follows are direct quotes from Regulatory Guide 5.71.

> 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.
>
> 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.

The following lists Records and supporting technical documentation in Regulatory Guide 5.71 required by the cyber security regulations.

The Regulatory Guide 5.71 requirements in **bold** are specific and those not in bold are not specific. Those that are not specific need to be clarified.

Records and supporting technical documentation required by the cyber security regulations	RG 5.71 requirements
Analysis of digital computer and communication systems and networks and **identification** of those assets that must be protected against cyber attacks	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.
Implementation, and maintenance of the cyber security program	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.
Incorporation the cyber security program as a component of the physical protection program	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.
Cyber Security Plan	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.
Design of the cyber security program to address specific items	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.
Traning	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.
Evaluation and management of cyber risks	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.
Modifications	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.
Cyber Security Plan	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.
Written policies and implementing procedures.	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.
Review of the cyber security program.	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.

The following lists records and supporting technical documentation in Regulatory Guide 5.71 NOT required by the cyber security regulations.

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.

1.8 RECOMMENDATIONS

The Records and supporting technical documentation required to be maintained, the Records retention section of NEI 08-09 and RG 5.71 was evaluated. Based upon the evaluation, it is recommended that NEI 08-09 be revised as follows:

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 will be retained 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:

Records and supporting technical documentation required by the cyber security regulations
Analysis of digital computer and communication systems and networks and identification of those assets that must be protected against cyber attacks
Implementation, and maintenance of the cyber security program
Incorporation the cyber security program as a component of the physical protection program
Cyber Security Plan
Design of the cyber security program
Training
Evaluation and management of cyber risks
Modifications
Cyber Security Plan
Written policies and implementing procedures.

Review of the cyber security program.

CDA audit records will be retained for no less than 12 months. CDA auditing capabilities are configured in accordance with section 3.1.6 of this plan.

Where a central logging server is employed, the audit records received will be retained for no less than 12 months.

The following audit data will be retained:
- Audit data described in Appendix D, 2.3, "Content of audit records"
- Audit data that support Appendix E, "Defense-in-Depth" security control will be retained to provide support for after-the-fact investigations of security attacks and satisfy the requirements of 10 CFR 73.54 and 10 CFR 73.55.

Audit (digital and non-digital) data include:
- Operating system logs
- Service and application logs
- Network device logs

For the purposes of this Plan, audit data is not required to be maintained under the QA Records Program.

The records and supporting technical documentation required to be maintained, the records retention section of NEI 08-09 and RG 5.71 was evaluated. Based upon the evaluation, it is recommended that NEI 08-09 be revised as follows:

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 , as follows:

Records and supporting technical documentation required by the cyber security regulations
Analysis of digital computer and communication systems and networks and identification of those assets that must be protected against cyber attacks
Implementation, and maintenance of the cyber security program
Incorporation the cyber security program as a component of the physical protection program
Cyber Security Plan
Design of the cyber security program
Training
Evaluation and management of cyber risks
Modifications
Cyber Security Plan
Written policies and implementing procedures.
Review of the cyber security program.

[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.