~~SECURITY-RELATED INFORMATION - WITHHOLD UNDER 10 CFR 2.390~~

Entergy Nuclear Northeast
Entergy Nuclear Operations, Inc.
James A. FitzPatrick NPP
P.O. Box 110
Lycoming, NY 13093
Tel 315-349-6024 Fax 315-349-6480

Kevin Bronson
Site Vice President - JAF

JAFP-11-0035
April 4, 2011

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

Subject: Response to Requests for Additional Information (RAIs) and Revision to the JAF Cyber Security Plan (TAC NO. ME4267)
James A. FitzPatrick Nuclear Power Plant
Docket Nos. 50-333
License Nos. DPR-59

References:

1. Entergy letter, License Amendment Withdrawal and Request – Cyber Security Plan, JAFP-10-0075, dated July 15, 2010.
2. Entergy letter, Clarification of JAF Cyber Security Plan Regarding Balance-of-Plant Systems within the Scope of the Program, JAFP-10-0142, dated November 30, 2010.
3. Letter from Richard P. Correia (NRC) to Chris Earls (NEI) Concerning Scope of Systems, dated January 5, 2011.
4. Entergy letter, Response to Request for Additional Information Regarding Application for Approval of the Cyber Security Plan, JAFP-11-0017, dated February 15, 2011.
5. Email from NRC to Entergy, RAI on License Amendment Request, Cyber Security Plan, dated February 23, 2011.
6. Letter from Chris Earls (NEI) to Richard P. Correia (NRC), Clarification to NEI 08-09, Revision 6 Regarding Records Retention, dated February 28, 2011.
7. Letter from Chris Earls (NEI) to Richard P. Correia (NRC), Template for the Cyber Security Plan Implementation Schedule, dated February 28, 2011.
8. Letter from Richard P. Correia (NRC) to Chris Earls (NEI), Cyber Security Plan Generic RAI on Records Retention, dated March 1, 2011.
9. Letter from Richard P. Correia (NRC) to Chris Earls (NEI), Template for the Cyber Security Plan Implementation Schedule, dated March 1, 2011.

Dear Sir or Madam:

Attachments 1, 4, and 6 contains Sensitive Unclassified Non-Safeguards Information.
When separated from Attachments 1, 4, and 6, this transmittal document is decontrolled.

Entergy Operations, Inc. (Entergy) submitted a request [Reference 1] for an amendment to the James A. FitzPatrick Nuclear Power Plant (JAF) operating license for NRC approval. In accordance with the previous Request for Additional Information (RAI) [Reference 4], Entergy is revising the JAF Cyber Security Plan Sections 2.1 "Scope and Purpose" and 4.3 "Defense-In-Depth Protective Strategies," to clarify data diodes/air gaps and emergency plan/preparedness as described in the RAI. Subsequent to the submittal of the RAI response, the NRC issued additional generic RAIs on the JAF Cyber Security Plan [Reference 5]. Entergy's response to these RAIs is provided in Attachment 1.

Attachment 2 contains proposed marked-up facility operating license (FOL) pages for the Physical Protection license condition for JAF to include the JAF Cyber Security Plan. Attachment 3 contains the proposed revised operating license pages. The marked-up pages in Attachment 2 and the revised pages in Attachment 3 replace, in their entirety, the pages previously submitted in Reference 1.

Attachment 6 provides a revised copy of the JAF Cyber Security Plan, Revision 0, which incorporates changes to Sections 2.1 "Scope and Purpose," 4.3 "Defense-In-Depth Protective Strategies," and 4.13 "Document Control and Records Retention and Handling." No other technical changes have been made to the JAF Cyber Security Plan. The enclosed JAF Cyber Security Plan replaces, in its entirety, the JAF Cyber Security Plan previously submitted in Reference 1. The changes discussed in this letter are clarifying or administrative and do not impact the conclusions of the No Significant Hazards consideration determination previously provided in Reference 1.

Entergy requests that Attachments 1, 4, and 6, which contain security-related information (SRI), be withheld from public disclosure in accordance with 10 CFR 2.390.

The revised commitments contained in this submittal are summarized in Attachment 5. Should you have any questions concerning this letter, or require additional information, please contact Joseph Pechacek, Licensing Manager, at 315-349-6766.

I declare under penalty of perjury that the foregoing is true and correct. Executed on April 4, 2011.

Sincerely,

Kevin Bronson
Site Vice President

KB/JP/mh

Attachments:
1. Response to Requests for Additional Information (contains SRI)
2. Proposed JAF Facility Operating License (FOL) Changes (mark-up)
3. Revised JAF Facility Operating License (FOL) Pages
4. Cyber Security Plan Implementation Schedule (contains SRI)
5. List of Regulatory Commitments
6. Revised JAF Cyber Security Plan (contains SRI)

cc: Mr. William Dean
Regional Administrator, Region I
U. S. Nuclear Regulatory Commission
475 Allendale Road
King of Prussia, PA 19406-1415

Mr. Bhalchandra Vaidya, Project Manager
Plant Licensing Branch I-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Mail Stop O-8-C2A
Washington, DC 20555-0001

Resident Inspector's Office
U.S. Nuclear Regulatory Commission
James A. FitzPatrick Nuclear Power Plant
P.O. Box 136
Lycoming, NY 13093

Mr. Paul Eddy (w/o Attachments 1, 4, and 6)
New York State Department
of Public Service
3 Empire Plaza, 10th Floor
Albany, NY 12223-1350

Document Component(s):
001 Transmittal Letter JAFP-11-0035
002 JAFP-11-0035 Attachments 2, 3, and 5
003 JAFP-11-0035 Attachments 1, 4, and 6 (Security-Related information)

Attachment 1

JAFP-11-0035

Response to Requests for Additional Information
(3 Pages)

JAFP-11-0035
Attachment 1

Response to Requests for Additional Information (RAIs)

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 three years after the record is superseded, unless otherwise specified by the Commission.

The licensee's cyber security plan 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:

Entergy has revised Section 4.13, "Document Control and Records Retention and Handling," of the JAF Cyber Security Plan in accordance with References 6 and 8 of the cover letter.

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 cyber security plan 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 (DBT).

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 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 cyber security plan 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 cyber security plan.

(b) Identify Critical Systems and CDAs, as described in Section 3.1.3, "Identification of Critical Digital Assets," of the cyber security plan.

(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 cyber security plan.

(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 cyber security plan.

(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 cyber security plan.

(h) Full implementation of the cyber security plan for all safety, security, and emergency preparedness functions.

Provide a revised cyber security plan 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 cyber security plan implementation schedule containing the key milestone dates.

Response:

Attachment 4 provides a revised Cyber Security Plan Implementation Schedule in accordance with References 7 and 9 of the cover letter which replaces, in its entirety, the implementation schedule previously submitted in JAFP-10-0075 [Reference 1].

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 DBT 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 JAF's Cyber Security Plan meets the requirements of 10 CFR 73.54 and the additional guidance provided by the NRC.

Response:

In accordance with References 2 and 3 of the cover letter Entergy has revised Section 2.1, "Scope and Purpose," of the JAF Cyber Security Plan to add the following paragraph:

> 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 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. 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.

Attachment 2

JAFP-11-0035

Proposed JAF Facility Operating License (FOL) Changes (mark-up)
(2 Pages)

FOL Page 3
FOL Page 5

(4) ENO pursuant to the Act and 10 CFR Parts 30, 40, and 70 to receive, possess, and use, at any time, any byproduct, source and special nuclear material without restriction to chemical or physical form, for sample analysis or instrument calibration; or associated with radioactive apparatus, components or tools..

(5) Pursuant to the Act and 10 CFR Parts 30 and 70, to possess, but not separate, such byproduct and special nuclear materials as may be produced by the operation of the facility.

C. This renewed operating license shall be deemed to contain and is subject to the conditions specified in the following Commission regulations in 10 CFR Chapter I: Part 20, Section 30.34 of Part 30, Section 40.41 of Part 40, Sections 50.54 and 50.59 of Part 50, and Section 70.32 of Part 70; and is subject to all applicable provisions of the Act and to the rules, regulations, and orders of the Commission now or hereafter in effect; and is subject to the additional conditions specified or incorporated below:

(1) Maximum Power Level

ENO is authorized to operate the facility at steady state reactor core power levels not in excess of 2536 megawatts (thermal).

(2) Technical Specifications

The Technical Specifications contained in Appendix A, as revised through Amendment No. ~~299~~, are hereby incorporated in the renewed operating license. The licensee shall operate the facility in accordance with the Technical Specifications.

(3) Fire Protection

ENO shall implement and maintain in effect all provisions of the approved fire protections program as described in the Final Safety Analysis Report for the facility and as approved in the SER dated November 20, 1972; the SER Supplement No. 1 dated February 1, 1973; the SER Supplement No. 2 dated October 4, 1974; the SER dated August 1, 1979; the SER Supplement dated October 3, 1980; the SER Supplement dated February 13, 1981; the NRC Letter dated February 24, 1981; Technical Specification Amendments 34 (dated January 31, 1978), 80 (dated May 22, 1984), 134 (dated July 19, 1989), 135 (dated September 5, 1989), 142 (dated October 23, 1989), 164 (dated August 10, 1990), 176 (dated January 16, 1992), 177 (dated February 10, 1992), 186 (dated February 19, 1993), 190 (dated June 29, 1993), 191 (dated July 7, 1993), 206 (dated February 28, 1994) and 214 (dated June 27, 1994); and NRC Exemptions and associated safety evaluations dated April 26, 1983, July 1, 1983, January 11, 1985, April 30, 1986, September 15, 1986 and September 10, 1992 subject to the following provision:

Safeguards Contingency Plan, Revision 0," submitted by letter dated October 26, 2004, as supplemented by letter dated May 17, 2006.

ENO shall fully implement in accordance with an NRC-approved implementation schedule and maintain in effect all provisions of the Commission-approved JAF Cyber Security Plan pursuant to 10 CFR 73.55(c)(6) and 10 CFR 73.54 (74 FR 13970) and to the authority of 10 CFR 50.90 and 10 CFR 50.54(p).

E. Power Uprate License Amendment Implementation

The licensee shall complete the following actions as a condition of the approval of the power uprate license amendment.

(1) Recirculation Pump Motor Vibration

Perform monitoring of recirculation pump motor vibration during initial Cycle 13 power ascension for uprated power conditions.

(2) Startup Test Program

The licensee will follow a startup testing program, during Cycle 13 power ascension, as described in GE Licensing Topical Report NEDC-31897P-1, "Generic Guidelines for General Electric Boiling Water Reactor Power Uprate." The Startup test program includes system testing of such process control systems as the feedwater flow and main steam pressure control systems. The licensee will collect steady-state operational data during various portions of the power ascension to the higher licensed power level so that predicted equipment performance characteristics can be verified. The licensee will do the startup testing program in accordance with its procedures. The licensee's approach is in conformance with the test guidelines of GE Licensing Topical Report NEDC-31897P-1, "Generic Guidelines for General Electric Boiling Water Reactor Power Uprate." June 1991 (proprietary), GE Licensing Topical Report NEDO-31897, "Generic Guidelines for General Electric Boiling Water Reactor Power Uprate." February 1992 (nonproprietary), and NEDC-31897P-AA, Class III (proprietary), May 1992.

(3) Human Factors

The licensee will review the results of the Cycle 13 startup test program to determine any potential effects on operator training. Training issues identified will be incorporated in Licensed Operator training during 1997. Simulator discrepancies identified will be addressed in accordance with simulator Configuration Management procedural requirements.

F. Additional Conditions

The Additional Conditions contained in Appendix C, as revised through Amendment No. 289, are herby incorporated into this renewed operating license. ENO shall operate the facility in accordance with the Additional Conditions.

Attachment 3

JAFP-11-0035

Revised JAF Facility Operating License (FOL) Page
(2 Pages)

FOL Page 3
FOL Page 5

(4) ENO pursuant to the Act and 10 CFR Parts 30, 40, and 70 to receive, possess, and use, at any time, any byproduct, source and special nuclear material without restriction to chemical or physical form, for sample analysis or instrument calibration; or associated with radioactive apparatus, components or tools..

(5) Pursuant to the Act and 10 CFR Parts 30 and 70, to possess, but not separate, such byproduct and special nuclear materials as may be produced by the operation of the facility.

C. This renewed operating license shall be deemed to contain and is subject to the conditions specified in the following Commission regulations in 10 CFR Chapter I: Part 20, Section 30.34 of Part 30, Section 40.41 of Part 40, Sections 50.54 and 50.59 of Part 50, and Section 70.32 of Part 70; and is subject to all applicable provisions of the Act and to the rules, regulations, and orders of the Commission now or hereafter in effect; and is subject to the additional conditions specified or incorporated below:

(1) Maximum Power Level

ENO is authorized to operate the facility at steady state reactor core power levels not in excess of 2536 megawatts (thermal).

(2) Technical Specifications

The Technical Specifications contained in Appendix A, as revised through Amendment No. , are hereby incorporated in the renewed operating license. The licensee shall operate the facility in accordance with the Technical Specifications.

(3) Fire Protection

ENO shall implement and maintain in effect all provisions of the approved fire protections program as described in the Final Safety Analysis Report for the facility and as approved in the SER dated November 20, 1972; the SER Supplement No. 1 dated February 1, 1973; the SER Supplement No. 2 dated October 4, 1974; the SER dated August 1, 1979; the SER Supplement dated October 3, 1980; the SER Supplement dated February 13, 1981; the NRC Letter dated February 24, 1981; Technical Specification Amendments 34 (dated January 31, 1978), 80 (dated May 22, 1984), 134 (dated July 19, 1989), 135 (dated September 5, 1989), 142 (dated October 23, 1989), 164 (dated August 10, 1990), 176 (dated January 16, 1992), 177 (dated February 10, 1992), 186 (dated February 19, 1993), 190 (dated June 29, 1993), 191 (dated July 7, 1993), 206 (dated February 28, 1994) and 214 (dated June 27, 1994); and NRC Exemptions and associated safety evaluations dated April 26, 1983, July 1, 1983, January 11, 1985, April 30, 1986, September 15, 1986 and September 10, 1992 subject to the following provision:

Safeguards Contingency Plan, Revision 0," submitted by letter dated October 26, 2004, as supplemented by letter dated May 17, 2006.

ENO shall fully implement in accordance with an NRC-approved implementation schedule and maintain in effect all provisions of the Commission-approved JAF Cyber Security Plan pursuant to 10 CFR 73.55(c)(6) and 10 CFR 73.54 (74 FR 13970) and to the authority of 10 CFR 50.90 and 10 CFR 50.54(p).

E. Power Uprate License Amendment Implementation

The licensee shall complete the following actions as a condition of the approval of the power uprate license amendment.

(1) Recirculation Pump Motor Vibration

Perform monitoring of recirculation pump motor vibration during initial Cycle 13 power ascension for uprated power conditions.

(2) Startup Test Program

The licensee will follow a startup testing program, during Cycle 13 power ascension, as described in GE Licensing Topical Report NEDC-31897P-1, "Generic Guidelines for General Electric Boiling Water Reactor Power Uprate." The Startup test program includes system testing of such process control systems as the feedwater flow and main steam pressure control systems. The licensee will collect steady-state operational data during various portions of the power ascension to the higher licensed power level so that predicted equipment performance characteristics can be verified. The licensee will do the startup testing program in accordance with its procedures. The licensee's approach is in conformance with the test guidelines of GE Licensing Topical Report NEDC-31897P-1, "Generic Guidelines for General Electric Boiling Water Reactor Power Uprate." June 1991 (proprietary), GE Licensing Topical Report NEDO-31897, "Generic Guidelines for General Electric Boiling Water Reactor Power Uprate." February 1992 (nonproprietary), and NEDC-31897P-AA, Class III (proprietary), May 1992.

(3) Human Factors

The licensee will review the results of the Cycle 13 startup test program to determine any potential effects on operator training. Training issues identified will be incorporated in Licensed Operator training during 1997. Simulator discrepancies identified will be addressed in accordance with simulator Configuration Management procedural requirements.

F. Additional Conditions

The Additional Conditions contained in Appendix C, as revised through Amendment No. 289, are herby incorporated into this renewed operating license. ENO shall operate the facility in accordance with the Additional Conditions.

Attachment 4

JAFP-11-0035

Cyber Security Plan Implementation Schedule
(4 Pages)

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 JAF Cyber Security Plan requires prioritization to assure those activities that provide higher degrees of protection against radiological sabotage are performed first. Therefore the cyber security plan 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 15, 2014, 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 JAF Cyber Security Plan.	No later than Dec. 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 JAF Cyber Security Plan.	No later than Dec. 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

#	Implementation Milestone	Completion Date	Basis
			preparedness functions. The scope of 10 CFR 73.54 also 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.
3	Implement installation of a deterministic one-way (or air gap) 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 JAF Cyber Security Plan. 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 Dec. 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	No later than	Portable media devices are used to

#	Implementation Milestone	Completion Date	Basis
	Control for Portable and Mobile Devices" described in Appendix D 1.19 of Nuclear Energy Institute (NEI) 08-09, Revision 6, will be implemented.	Dec. 31, 2012	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 Appendix E Section 4.3 "Personnel Performing Maintenance and Testing Activities" of NEI 08-09, Revision 6.	No later than Dec. 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 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	No later than Dec. 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 security controls to target set CDAs provides a high degree of protection against a 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.

#	Implementation Milestone	Completion Date	Basis
	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 Section 4.4, “Ongoing Monitoring and Assessment” of the JAF Cyber Security Plan, for those target set CDAs whose security controls have been implemented.	No later than Dec. 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 JAF Cyber Security Plan for all SSEP functions will be achieved.	Dec. 15, 2014	By the completion date, the JAF 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 refueling outage for implementation.

Attachment 5

JAFP-11-0035

List of Regulatory Commitments
(1 Page)

List of Regulatory Commitments

The following table identifies those actions committed to by Entergy in this document. Any other statements in this submittal are provided for information purposes and are not considered to be regulatory commitments.

COMMITMENT	TYPE (Check One)		SCHEDULED COMPLETION DATE (If Required)
	ONE-TIME ACTION	CONTINUING COMPLIANCE	
Entergy will implement milestones 1 through 7 of the Cyber Security Plan described in Attachment 4 of JAFP-11-0035.	X		December 31, 2012 Commitment 18435
Full implementation of JAF Cyber Security Plan for all safety, security, and emergency preparedness functions will be achieved.	X		December 15, 2014 Commitment 18436

Attachment 6

JAFP-11-0035

Revised JAF Cyber Security Plan
(23 Pages)

James A. FitzPatrick
CYBER SECURITY PLAN

1 INTRODUCTION

The purpose of this Cyber Security Plan (Plan) is to provide a description of how the requirements of 10 CFR 73.54, "Protection of digital computer and communication systems and networks" (Rule) are implemented at James A. FitzPatrick (JAF). The intent of this Plan is to protect the health and safety of the public from radiological sabotage as a result of a cyber attack as described in 10 CFR 73.1. 10 CFR 50.34(c), "Physical Security Plan," requires the inclusion of a physical security plan. JAF acknowledges that the implementation of this plan does not alleviate their responsibility to comply with other NRC regulations.

Further, 10 CFR 50.34(c)(2) states in part that "Each applicant for an operating license for a utilization facility that will be subject to the requirements of 10 CFR 73.55 of this chapter must include a cyber security plan in accordance with the criteria set forth in 10 CFR 73.54 of this chapter." This Cyber Security Plan establishes the licensing basis for the Cyber Security Program (Program) for JAF.

A Glossary of terms used within this Plan and Appendices of Nuclear Energy Institute (NEI) 08-09, Revision 6, is contained in Appendix B of NEI 08-09, Revision 6.

2 CYBER SECURITY PLAN

2.1 SCOPE AND PURPOSE

This Plan establishes a means to achieve high assurance that digital computer and communication systems and networks associated with the following functions (hereafter designated as Critical Digital Assets (CDAs)) are adequately protected against cyber attacks up to and including the Design Basis Threat (DBT) as described in 10 CFR 73.1:

1. Safety-related and important-to safety functions;
2. Security functions;
3. Emergency preparedness functions including offsite communications; and
4. Support systems and equipment which if compromised, would adversely impact safety, security, or emergency preparedness functions.

The safety-related and important-to safety functions, security functions, and emergency preparedness functions including offsite communications are herein referred to as Safety, Security, and Emergency Preparedness (SSEP) functions.

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.

High assurance of adequate protection of systems associated with the above functions from cyber attacks is achieved by:

1. Implementing and documenting the "baseline" cyber security controls described in Section 3.1.6 of this Plan; and
2. Implementing and documenting a cyber security program to maintain the established cyber security controls through a comprehensive life cycle approach as described in Section 4 of this Plan.

2.2 PERFORMANCE REQUIREMENTS

10 CFR 73.55(a)(1) requires that licensees implement the requirements of this section through its Commission-approved Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plans, and Cyber Security Plan, referred to collectively as "security plans."

As required by 10 CFR 73.54(b)(3), cyber security is a component of the physical protection program. As such, this Plan establishes how digital computer and communication systems and networks within the scope of 10 CFR 73.54 are adequately protected from cyber attacks up to and including the DBT characteristics described in Regulatory Guide (RG) 5.69, "Guidance for the Application of the Radiological Sabotage DBT in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements." (Safeguards Information).

Performance based requirements demonstrated in this Plan are designed to:

2.2.1 Evaluate modifications to CDAs prior to implementation to achieve high assurance that digital computer and communications systems and networks are adequately protected against cyber attacks, up to and including the DBT.

(10 CFR 73.54(a)(1) and 10 CFR 73.54(d)(3))

2.2.2 Prevent adverse impact to SSEP functions resulting from cyber attacks, that would adversely impact the integrity or confidentiality of data and/or software, deny access to systems, services, and/or data, and adversely impact the operation of systems, networks, and associated equipment to protect against the DBT.

(10 CFR 73.54(a)(2) and 10 CFR 73.55(b)(2))

2.2.3 Analyze digital computer and communications systems and networks and identify those assets that must be protected against cyber attack to preserve the intended function of plant systems, structures, and components within the scope of the Rule and account for these conditions in the design of the Program.

(10 CFR 73.54(b)(1) and 10 CFR 73.55(b)(4))

2.2.4 Establish, implement and maintain the Program in accordance with 10 CFR 73.54.

(10 CFR 73.54(b)(2) and 10 CFR 73.55(b)(8))

2.2.5 Incorporate the cyber security program as a component of the physical protection program.

(10 CFR 73.54(b)(3) and 10 CFR 73.55(b)(8))

2.2.6 Implement security controls to protect the identified assets from cyber attacks.

(10 CFR 73.54(c)(1))

2.2.7 Provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure effectiveness of the Program.

(10 CFR 73.54(c)(2) and 10 CFR 73.55(b)(3)(ii))

2.2.8 Maintain the capability to mitigate the adverse consequences of cyber attacks.

(10 CFR 73.54(c)(3) and 10 CFR 73.54(e)(2)(ii))

2.2.9 Ensure that the functions of identified protected assets are not adversely impacted due to cyber attacks.

(10 CFR 73.54(c)(4))

2.2.10 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.

(10 CFR 73.54(d)(1))

2.2.11 Use the site corrective action program to: 1) track, trend, correct, and prevent recurrence of cyber security failures and deficiencies, and 2) evaluate and manage cyber risks.

(10 CFR 73.54(d)(2) and 10 CFR 73.55(b)(10))

2.2.12 Describe how the cyber security program requirements will be implemented; accounting for the site-specific conditions that affect implementation.

(10 CFR 73.54(e)(1))

2.2.13 Ensure that the Program maintains the capability to detect, respond to, and recover from cyber attacks up to and including the DBT of radiological sabotage as stated in 10 CFR 73.1 at all times.

(10 CFR 73.54(e)(2)(i), 10 CFR 73.54(e)(2)(iv) and 10 CFR 73.55(b)(2))

2.2.14 Maintain the capability to correct exploited vulnerabilities.

(10 CFR 73.54(e)(2)(iii))

2.2.15 Demonstrate the ability to meet Commission requirements through implementation of the Program in licensee policies and procedures which are available upon the request of an authorized representative of the Commission.

(10 CFR 73.54(f) and 10 CFR 73.55(b)(5))

2.2.16 Review the cyber security program as a component of the physical security program, including the periodicity requirements.

(10 CFR 73.54(g) and 10 CFR 73.55(m))

2.2.17 Describe how all records and supporting technical documentation are retained.

(10 CFR 73.54(h))

2.2.18 Coordinate implementation of this Plan and associated procedures with other JAF and Entergy fleet-wide procedures to preclude conflict during both normal and emergency conditions.

(10 CFR 73.55(b)(11))

3 ANALYZING DIGITAL COMPUTER SYSTEMS AND NETWORKS

The Cyber Security Program is established, implemented, and maintained in accordance with 10 CFR 73.54(b)(2) and 10 CFR 73.55(b)(8) to protect those systems required by 10 CFR 73.54(a)(1)(i–iv) from cyber attacks that would: adversely impact the integrity or confidentiality of data and/or software; deny access to systems, services and/or data; or adversely impact the operation of systems, networks, and associated equipment. This Cyber Security Program complies with 10 CFR 73.54 by implementing cyber security controls, defensive strategies, and attack mitigation methods that meet the Rule.

The cyber security controls described in Appendices D and E of NEI 08-09, Revision 6, are implemented in accordance with Section 3.1.6 of this Plan. Documentation of the cyber security controls in place for CDAs are not submitted with this Plan but are available on site for inspection by the NRC. Cyber security program changes that are determined to decrease the effectiveness of this Plan are submitted to the NRC for approval as required by 10 CFR 50.90. Revisions to this Plan are processed in accordance with procedures that implement the requirements of 10 CFR 50.54(p). Cyber attacks at JAF are reported to the NRC in accordance with the requirements of 10 CFR 73, Appendix G.

3.1 ANALYZING DIGITAL COMPUTER SYSTEMS AND NETWORKS AND APPLYING CYBER SECURITY CONTROLS

In accordance with 10 CFR 73.54(b)(1), the Cyber Security Program is established, implemented, and is maintained to:

- Analyze digital computer and communications systems and networks, and
- Identify those assets that must be protected against cyber attacks to satisfy 10 CFR 73.54(a).

In accordance with 10 CFR 73.54(c)(1), cyber security controls are implemented to protect the assets identified by 10 CFR 73.54(b)(1) from cyber attacks. The cyber security controls provided in Appendices D and E of NEI 08-09, Revision 6, are used as the basis for protecting the identified CDAs.

Cyber security risks are evaluated, managed, and mitigated to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks up to and including the DBT. The cyber security controls provided in Appendices D and E of NEI 08-09, Revision 6, are the technical, operational, and management countermeasures available to protect the availability, integrity, and confidentiality of CDAs. The cyber security controls in Appendices D and E of NEI 08-09, Revision 6, are implemented using the methodology in Sections 3.1.1 through 3.1.6 below. In so doing, high assurance of adequate protection of CDAs associated with SSEP functions from cyber attacks defined by 10 CFR 73.1 and RG 5.69 is ensured.

3.1.1 Cyber Security Assessment and Authorization

JAF develops, disseminates, periodically reviews in accordance with 10 CFR 73.55(m), and updates:

- A formal, documented, cyber security assessment and authorization procedure that defines and addresses: the purpose, scope, roles, responsibilities, management commitment, and coordination among departments; and the implementation of the cyber security controls in Appendices D and E of NEI 08-09, Revision 6.
- A formal, documented procedure to facilitate the implementation of the cyber security assessment.

3.1.2 Cyber Security Assessment Team

A Cyber Security Assessment Team (CSAT) is formed consisting of individuals with broad knowledge in the following areas:

- Information and digital system technology – This includes cyber security, software development, offsite communications, computer system administration, computer engineering and computer networking. Knowledge of the digital systems involved in plant operations, including digital instrumentation and control systems, and those involved in plant information systems, is included. Plant operational systems include programmable logic controllers, control systems, and distributed control systems. Information systems include computer systems and databases containing information used to design, operate, and maintain CDAs. In the networking arena, knowledge of both plant- and corporate-wide networks is included.
- Nuclear power plant operations, engineering, and nuclear safety – This includes overall facility operations and plant technical specifications. The staff representing this technical area has the ability to trace the impact of a vulnerability or series of vulnerabilities in a CDA (or connected digital asset) outward through plant systems and subsystems so that the overall impact on SSEP functions of the plant can be evaluated.
- Physical security and emergency preparedness – This includes the site's physical security and emergency preparedness systems and programs.

The roles and responsibilities of the CSAT include such activities as:

- Performing or overseeing stages of the cyber security assessment process.
- Documenting key observations, analyses, and findings during the assessment process.
- Evaluating assumptions and conclusions about cyber security threats; potential vulnerabilities to, and consequences from an attack; the effectiveness of existing cyber security controls, defensive strategies, and attack mitigation methods; cyber security awareness and training of those working with, or responsible for CDAs and cyber security controls throughout their system life cycles; and estimates of cyber security risk levels.
- Confirming information acquired during tabletop reviews by conducting walk-downs or electronic validation of CDAs and connected digital assets, and associated cyber security controls.

- Identifying potential new cyber security controls.
- Documenting the required cyber security control application per Section 3.1.6 of this Plan.
- Transmitting assessment documentation, including supporting information, to Records Management in accordance with 10 CFR 73.54(h) and the record retention requirements specified in Section 4.13 of this Plan.

The CSAT has the authority to conduct an assessment in accordance with the requirements of Section 3 of this Plan.

3.1.3 Identification of Critical Digital Assets

The CSAT:

- Identifies and documents Critical Systems (CS), which must be protected under the Rule. (Refer to NEI 08-09, Revision 6, Appendix B, Glossary for definition of Critical System).
- Identifies and documents Critical Digital Assets (CDAs). (Refer to NEI 08-09, Revision 6, Appendix B, Glossary for definition of Critical Digital Asset).

The process by which CDAs are identified has been documented.

For each CS examined, the documentation includes the following:

- Identification of the Critical System;
- Identification of the digital devices that provide direct or supporting roles in the function of the CS (e.g., protection, control, monitoring, reporting, or communications);
- Identification of CDAs within the Critical System;
- General description of the CDAs;
- Brief description of overall function of the CDAs;
- Description of overall consequence to the CS and SSEP functions if a compromise of the CDA occurs; and
- Security functional requirements or specifications, as available, that include the following:
    - Information security requirements necessary for vendors and developers to maintain the integrity of acquired systems;
    - Secure configuration, installation, and operation of the CDA;
    - Effective use and maintenance of security features/functions;
    - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
    - User-accessible security features/functions and how to effectively use those security features/functions;
    - Methods for user interaction with CDAs, which enables individuals to use the system in a more secure manner; and
    - User responsibilities in maintaining the security of the CDA.

3.1.4 Examination of Cyber Security Practices

The CSAT collects, examines, and documents the existing cyber security policies, procedures, and practices; existing cyber security controls; detailed descriptions of network and communication architectures (or network/communication architecture drawings); information on security devices; and any other information that may be helpful during the cyber security assessment process. The team collects, documents by reference, and evaluates the following as they apply to CDAs:

- Site and corporate-wide information on defensive strategies including cyber security controls, defensive models, and other defensive strategy measures;
- The site's physical and operational security program with respect to the protection of CDAs;
- Site and corporate network architectures, and configuration information on security devices;
- Cyber security requirements for vendors and contractors while on site or used during procurement;
- Information on computer networks and communication systems and networks that are present within the plant and could be potential pathways for attacks;
- Cyber security assessments, studies, evaluations or audits to gain insight into areas of potential vulnerabilities; and
- Infrastructure support systems (e.g., electrical power; heating, ventilation, and air conditioning; communications; fire suppression) which, if compromised, could adversely impact the proper functioning of CDAs.

The examination includes an analysis of the effectiveness of existing cyber security programs and cyber security controls. The CSAT documents the collected cyber security information and the results of their examination of the collected information.

3.1.5 Tabletop Reviews and Validation Testing

The CSAT conducts a tabletop review and validation activities.

Results of table top reviews and validation reviews are documented.

For each CDA/CDA group, the CSAT:

- Confirms the location;
- Confirms direct and indirect connectivity pathways;
- Confirms infrastructure interdependencies;
- Reviews any CDA assessment documentation;
- Reviews the defensive strategies;
- Reviews the defensive models;

- Confirms the implementation of plant-wide physical and cyber security policies and procedures that secure the CDAs from a cyber attack, including attack mitigation, and incident response and recovery;
- Confirms that staff members working with the CDAs are trained to a level of cyber security knowledge commensurate with their assigned responsibilities; and
- Identifies and documents the CDA cyber security exposures including specific attack/threat vectors to be assessed for mitigation using the method in Section 3.1.6.

The above activities are validated for CDAs through walk-downs. These walk-downs include:

- Performing, where practical, a physical inspection of the connections and configuration of CDAs, including tracing communication connections into and out of the CDA to termination points along communication pathways.
- Performing electronic validation when physical walk-down inspections are impractical to trace a communication pathway to its conclusion. When there is a risk of operational disruption, electronic validation tests are conducted during periods of scheduled outage. Where used, a justification of the adequacy of the electronic validation technique is documented.
- Examining the physical security established to protect CDAs and the CDA's communication pathways.
- Examining the configuration and assessing the effectiveness of cyber security controls (e.g., firewalls, intrusion detection systems, data diodes) along the communication pathways.
- Examining interdependencies with other CDA(s) and trust relationships between the CDA(s).
- Examining interdependencies with infrastructure support systems including electrical power, environmental controls, and fire suppression equipment which, if compromised, could adversely impact the proper functioning of CDAs.
- Resolving information and/or configuration discrepancies identified during the tabletop reviews, including the presence of undocumented and/or missing connections, and other cyber security-related irregularities associated with the CDA.

Information and/or configuration discrepancies identified during the tabletop reviews and walk-downs, including the presence of undocumented and/or missing connections, and other cyber security-related irregularities associated with the CDA are documented for remediation in the Corrective Action Program.

3.1.6 Mitigation of Vulnerabilities and Application of Cyber Security Controls

Defense-in-depth strategies are established by documenting and implementing the:

- Defensive strategy described in Section 4.3;
- Technical cyber security controls in Appendix D of NEI 08-09, Revision 6, consistent with the process described below; and

- Operational and Management cyber security controls in Appendix E of NEI 08-09, Revision 6, consistent with the process described below.

The CSAT utilizes the information gathered in Sections 3.1.3 through 3.1.5 to document how each of the technical cyber security controls were addressed for each CDA using the process described below. Other plant organizations may be used to implement the CSAT recommendations. For example, the Plant/Design Engineering group will perform requisite modifications to CDAs.

Cyber security controls are not applied if the control adversely impacts safety and important to safety, security or emergency preparedness functions. When a cyber security control is determined to have an adverse effect, alternate controls are used to mitigate the lack of the security control for the CDA per the process described in this section.

For CDAs, the information in Sections 3.1.3 - 3.1.5 is utilized to analyze and document one or more of the following:

1. Implementing the cyber security controls in Appendices D and E of NEI 08-09, Revision 6.
2. Implementing alternative controls/countermeasures that eliminate threat/attack vector(s) associated with one or more of the cyber security controls enumerated in (1) above by:
    a. Documenting the basis for employing alternative countermeasures;
    b. Performing and documenting the analyses of the CDA and alternative countermeasures to confirm that the countermeasures provide the same or greater cyber security protection as the corresponding cyber security control;
    c. Implementing alternative countermeasures that provide at least the same degree of cyber security protection as the corresponding cyber security control; and
    d. Implementing an alternative frequency or periodicity for the security control employed by documenting the basis for the alternate frequency or periodicity. The basis incorporates one or more of the following:
        i. NRC Regulations, Orders
        ii. Operating License Requirements (e.g., Technical Specifications)
        iii. Site operating history
        iv. Industry operating experience
        v. Experience with security control
        vi. Guidance in generally accepted standards (e.g., National Institute of Standards and Technology, Institute of Electrical and Electronics Engineers, International Organization for Standardization)
        vii. Audits and Assessments
        viii. Benchmarking
        ix. Availability of new technologies.

3. Not implementing one or more of the cyber security controls by:

    a. Performing an analysis of the specific cyber security controls for the CDA that will not be implemented

    b. Documenting justification demonstrating the attack vector does not exist (i.e., not applicable) thereby demonstrating that those specific cyber security controls are not necessary.

3.2 RECORDS

Records of the assessment described in Section 3.1 of this Plan are maintained in accordance with approved procedures as described in Section 4.13 of this Plan.

4 ESTABLISHING, IMPLEMENTING, AND MAINTAINING THE CYBER SECURITY PROGRAM

This section establishes the programmatic elements necessary to maintain cyber security throughout the life cycle of CDAs. The elements of this section are implemented to maintain high assurance that CDAs associated with the SSEP functions are adequately protected from cyber attacks up to and including the DBT.

A life cycle approach is employed consistent with the controls described in Appendix E of NEI 08-09, Revision 6. This approach ensures that the cyber security controls established and implemented for CDAs are maintained to achieve the site's overall cyber security program objectives. For proposed new digital assets, or existing digital assets that are undergoing modification, the process described in Sections 10 and 11 of the Operational and Management controls of NEI 08-09, Revision 6, Appendix E are implemented.

Records are maintained in accordance with Section 4.13 of this Plan.

4.1 INCORPORATING THE CYBER SECURITY PROGRAM INTO THE PHYSICAL PROTECTION PROGRAM

The Cyber Security Program, which is referenced in the Physical Security Plan, implements the Cyber Security Program requirements in accordance with 10 CFR 73.54(b)(3), 10 CFR 73.55(a)(1), and 10 CFR 73.55(c)(6). Cyber attacks are also considered during the development and identification of target sets as required by the Physical Security Program and 10 CFR 73.55(f)(2).

Revisions to this Plan are processed in accordance with procedures that implement the requirements of 10 CFR 50.54(p). Changes that are determined to decrease the effectiveness of this Plan are submitted to the NRC for approval as required by 10 CFR 50.90.

The Cyber Security Program is reviewed as a component of the Physical Security Program as required by 10 CFR 73.55(m).

4.2 CYBER SECURITY CONTROLS

The Technical, Operational and Management Cyber Security Controls described in Appendices D and E of NEI 08-09, Revision 6, are evaluated and dispositioned based on site specific conditions during the establishment of risk baselines, during on-going programs, and during oversight activities.

Cyber security controls are used to protect CDAs within the scope of the Rule. The cyber security controls are implemented utilizing the process described in Section 3.1.6 of this Plan.

Management controls, Operational controls, and Technical controls, in conjunction with Physical Security Plans, support the overall safety of nuclear material and reliability of plant operations. The Cyber Security Controls are utilized in the site Baseline Assessment, Configuration Management, Engineering Design Control, Training, Attack Mitigation, and Incident Response, Record Retention and Handling, and Review programs.

If a CDA cannot support the use of automated cyber security control mechanisms, non-automated cyber security control mechanisms or procedures are documented and utilized where necessary to maintain the desired level of protection.

Many security controls have actions that are required to be performed on specific frequencies. The frequency of a security control is met if the action is performed within 1.25 times the frequency specified in the control, as applied, and as measured from the previous performance of the action. This extension facilitates scheduling and considers plant operating conditions that may not be suitable for conducting the security control action (e.g., transient conditions, other ongoing surveillance or maintenance activities). These provisions are not intended to be used repeatedly merely as an operational convenience to extend frequencies beyond those specified.

4.3 DEFENSE-IN-DEPTH PROTECTIVE STRATEGIES

Defense-in-depth protective strategies have been implemented, documented, and are maintained to ensure the capability to detect, delay, respond to, and recover from cyber attacks on CDAs. The defensive strategy describes the defensive security architecture, identifies the protective controls associated within each security level, implements cyber security controls in accordance with Section 3.1 of this Plan, employs the Defense-in-Depth measures described in NEI 08-09, Appendix E, Section 6, and maintains the cyber security program in accordance with in Section 4 of this Plan.

The defensive architecture has been implemented, documented, and is maintained to protect CDAs that have similar cyber risks from other CDAs, systems or equipment by establishing the logical and physical boundaries to control the data transfer between boundaries.

This defensive architecture provides for cyber security defensive levels separated by security boundaries devices, such as firewalls and diodes, at which digital communications are monitored and restricted. Systems requiring the greatest degree of security are located within the greatest number and strength of boundaries. The criteria below are utilized in the defensive architecture.

The site defensive model implements all of the following:

- The defensive model consists of a four-level layered approach, with increasing electronic security from Level 1 up to Level 4. Each level is electronically protected or isolated from the levels below it by a lower security boundary consisting of one or more measures described below. The open internet is below Level 1. Level 4 has the strongest degree of security. In addition to electronic security measures, physical barriers and access controls are employed, as described in NEI 08-09, Revision 6, Appendices D and E, and the Physical Security Plan.
- CDAs that perform safety control and safety support functions, security control and security support functions, and safety and security data acquisition are within Level 4. The lower electronic security boundary of Level 4 is an air gap or deterministic one-way isolation device such as a data diode.
- CDAs that are not required to be within Level 4 due to their safety or security significance, and that perform security or emergency preparedness functions and security or emergency preparedness data acquisition or that perform safety monitoring, are within Level 3. The lower electronic security boundary of Level 3 is a firewall and an intrusion detection system or similar control per NEI 08-09, Revision 6, Appendix D, Section 1.4 and Appendix E, Section 6 (except that for specifically authorized connections two-way data flow is allowed), or an air gap or deterministic one-way isolation device such as a data diode.
- CDAs that are not required to be in at least Level 3 and that perform or support emergency preparedness functions are within Level 2. The lower electronic security boundary of Level 2 is a firewall and intrusion detection system or similar control per NEI 08-09, Revision 6, Appendix D, Section 1.4 and Appendix E, Section 6 (except that for specifically authorized connections two-way data flow is allowed), or an air gap or deterministic one-way isolation device such as a data diode.
- The site local area network is within Level 2 and the corporate wide area network is within Level 1. The lower electronic security boundary of Level 1 is a firewall and intrusion detection system and is controlled per corporate information security policies.

For this defensive architecture to be effective in protecting CDAs from cyber attacks the above characteristics are consistently applied, along with the technical, management, and operational security controls discussed in Appendices D and E of NEI 08-09, Revision 6.

The cyber security defensive model is enhanced by physical and administrative cyber security controls implemented by the Physical Security Program. Physical barriers such as locked doors, locked cabinets, and/or locating CDAs in the protected area or vital area are also used to mitigate risk.

4.4 ONGOING MONITORING AND ASSESSMENT

Ongoing monitoring of cyber security controls used to support CDAs is implemented consistent with Appendix E of NEI 08-09, Revision 6. Automated support tools are also used, where available, to accomplish near real-time risk management for CDAs. The ongoing monitoring program includes:

- Configuration management of CDAs;
- Cyber security impact analyses of changes to the CDAs or their environment(s) to ensure that implemented cyber security controls are performing their functions effectively;
- Ongoing assessments to verify that the cyber security controls implemented for CDAs remain in place throughout the life cycle of the CDA;
- Verification that rogue assets are not connected to the network infrastructure;
- Ongoing assessments of the need for and effectiveness of the cyber security controls identified in Appendices D and E of NEI 08-09, Revision 6; and
- Periodic cyber security program review to evaluate and improve the effectiveness of the Program.

This element of the Program is mutually supportive of the activities conducted to monitor configuration changes of CDAs.

4.4.1 Configuration Management and Change Control

The configuration management controls described in Appendix E of NEI 08-09, Revision 6, have been implemented as described in Section 3.1.6, and implementation has been documented. A configuration management approach is implemented to update and maintain cyber security controls for CDAs in order to ensure that the cyber security program objectives remain satisfied. Modifications to CDAs are evaluated before implementation to ensure that the cyber security performance objectives of 10 CFR 73.54(a)(1) are maintained. A record of changes made to the configuration of CDAs is maintained.

CDA cyber security and configuration management documentation is updated or created using the site configuration management program or other configuration management procedure or process. This documentation includes the bases for not implementing one or more of the technical cyber security controls specified in Appendix D of NEI 08-09, Revision 6.

During the operation and maintenance phases of the CDA life cycle, changes to CDAs are made using design control, Software Quality Assurance, and configuration management procedures, so that additional cyber security risk is not introduced into the system. The process ensures that the controls specified in Appendices D and E of NEI 08-09, Revision 6, have been implemented in a manner consistent with this Plan and implementing procedures.

During the retirement phase, the design control and Configuration Management procedures address SSEP functions.

4.4.2 Cyber Security Impact Analysis of Changes and Environment

A cyber security impact analysis is performed prior to making a design or configuration change to a CDA, or when changes to the environment occur, consistent with the process described in Section 4 of the Operational and Management Controls of Appendix E to NEI 08-09, Revision 6, to manage risks introduced by the changes.

Interdependencies of other CDAs or support systems are evaluated, documented, and incorporated into the cyber security impact analysis. The steps for conducting the tabletop review described in Section 3.1.5 are performed.

These impact analyses are performed as part of the change approval process to assess the impacts of the changes on the cyber security posture of CDAs and systems that can affect SSEP functions. Cyber security related issues identified during the change management process are addressed within the change management process, and therefore are not handled by the Corrective Action Program. Adverse conditions identified after the modification is implemented are entered into the site Corrective Action Program.

Risks to SSEP functions, CDAs and CSs are managed through ongoing evaluation of threats and vulnerabilities and by addressing threat and attack vectors associated with the cyber security controls provided in Appendices D and E of NEI 08-09, Revision 6, during the various phases of the life cycle. Additionally, procedures are developed for screening, evaluating, mitigating and dispositioning threat and vulnerability notifications received from credible sources. Dispositioning includes implementation, as necessary, of cyber security controls to mitigate newly reported or discovered vulnerabilities and threats.

4.4.3 Ongoing Assessment of Cyber Security Controls

Ongoing assessments are performed to verify that the cyber security controls implemented for CDAs remain in place throughout the life cycle. The assessment process verifies the status of these cyber security controls at least every 24 months or in accordance with the specific requirements for utilized cyber security controls as described in Appendices D and E of NEI 08-09, Revision 6, whichever is more frequent.

4.4.3.1 Effectiveness Analysis

The effectiveness and efficiency of the Cyber Security Program and the cyber security controls in Appendices D and E of NEI 08-09, Revision 6, are monitored to confirm that the cyber security controls are implemented correctly, operating as intended, and continue to provide high assurance that CDAs are protected against cyber attacks up-to and including the DBT. Reviews of the cyber security program and controls include, but are not limited to, periodic audits of the physical security program, security plans, implementing procedures, cyber security programs; safety/security interface activities; the testing, maintenance, and calibration program as it relates to cyber security; and feedback from the NRC and local, state, and federal law enforcement authorities.

The effectiveness evaluation provides information for cyber security decision makers about the results of previous policy and acquisition decisions. These measures include:

- Provide insight for improving performance of the Cyber Security Program;
- Assist in determining the effectiveness of cyber security controls in Appendices D and E of NEI 08-09, Revision 6;
- Assist in ascertaining whether specific cyber security controls are functioning and are helping facilitate corrective action prioritization; and
- Require fusing the Cyber Security Program activities data with the data obtained from automated monitoring and evaluation tools in a manner that can be tied to cyber security control implementation.

The effectiveness of these cyber security controls is verified when applied, and at least every 24 months or in accordance with the specific requirements for employed cyber security controls as described in Appendices D and E of NEI 08-09, Revision 6, whichever is more frequent. Documents of maintenance and repairs on CDA components are reviewed to ensure that CDAs which perform cyber security functions are maintained according to recommendations provided by the manufacturer or as determined by site-specific procedures.

Adverse conditions identified during effectiveness evaluations are entered in the site Corrective Action Program.

4.4.3.2 Vulnerability Scans

Electronic vulnerability scanning of CDAs is performed when security controls are first applied, and as required by specific guidance in the cyber security controls in Appendices D and E of NEI 08-09, Revision 6. When new vulnerabilities that could affect the cyber security posture of CDAs are identified, vulnerability scanning will be performed.

Vulnerability scan reports are analyzed and vulnerabilities that could result in a risk to SSEP functions at the site are remediated. Information obtained from the vulnerability scanning process is shared with appropriate personnel to ensure that similar vulnerabilities that may impact interconnected or similar CDA(s) are understood, evaluated and mitigated.

When there is a risk of operational disruption, electronic vulnerability scans are conducted during periods of scheduled outage. Test beds and vendor maintained environments may be used for or in substitution for performing vulnerability scans.

Assessment and scanning processes must not adversely impact SSEP functions. If this could occur, CDAs are removed from service or replicated (to the extent feasible) before assessment and scanning is conducted. If vulnerability assessments or scanning cannot be performed on a production CDA because of the potential for an adverse impact on SSEP functions, alternate controls (e.g., providing a replicated system or CDA to conduct scanning) are employed.

A vulnerability assessment may be used as a substitute for vulnerability scanning where there is risk of an adverse impact to SSEP functions, and when off-line, replicated, or vendor test beds are not available. When new vulnerabilities are discovered, the vulnerability assessment considers the same threat vectors as the identified vulnerabilities. When vulnerability

assessments are used to verify security controls, the assessment targets the threat vectors the security controls address. In both cases, the vulnerability assessment verifies that the vulnerability or threat vector is addressed to provide high assurance of adequate protection that SSEP functions are protected from cyber attacks up-to and including the DBT.

4.5 ADDITION AND MODIFICATION OF DIGITAL ASSETS

The approach for assessing new/modified CDAs is to use the assessment process described in Section 3.1 of this Plan.

Design control and Software Quality Assurance program procedures have been established, implemented, and maintained to control life cycle phase activity cyber security controls for CDAs. These program procedures ensure that modifications to a CDA within the scope of 10 CFR 73.54 are evaluated before implementation to ensure that the cyber security performance objectives of 10 CFR 73.54(a)(1) are maintained and that acquired CDAs have cyber security requirements developed to achieve the site's cyber security program objectives.

Records are maintained in accordance with Section 4.13 of this Plan.

4.6 ATTACK MITIGATION AND INCIDENT RESPONSE

The Program ensures that the Safety, Security, and Emergency Preparedness functions of digital assets within the scope of the Rule (CDAs) are not adversely impacted due to cyber attacks. Appendix E of NEI 08-09, Revision 6, includes the following topics pertaining to attack mitigation and incident response:

- Incident Response Policy and Procedures
- Incident Response Training
- Incident Response Testing and Drills
- Incident Handling
- Incident Monitoring
- Incident Response Assistance

Cyber Security Program procedures document cyber security controls to deny, deter, and detect adverse threats and conditions to CDAs that may be susceptible to cyber attacks which exploit system vulnerabilities. Cyber security controls employed counteract threats. Cyber Security Program procedures document the methods to handle digital-related adverse conditions.

Digital-related adverse conditions are entered into the site Corrective Action Program for resolution. If the condition affects a CDA, the condition is evaluated to determine if there is reason to believe that the condition is the result of a cyber attack. If there is reason to believe the condition is the result of a cyber attack, the event is reported to the NRC in accordance with 10 CFR 73, Appendix G.

Identification, detection, and response to cyber attacks are directed by site procedures for cyber security and other procedures that govern response to plant events. When there is reasonable suspicion of a cyber attack, response instructions direct notification to the Shift Manager

Operations, Site Security Manager, and activation of Cyber Security Incident Response Team (CSIRT). Response instructions direct other emergency response actions, if warranted.

Cyber security attack containment activities are directed by site procedures. These measures include but are not limited to:

- Assist in determining the CDA's operability or functionality;
- Isolate the affected CDA with approval by Shift Manager, Operations, if possible; and
- Verify surrounding networks and support systems are not contaminated.

Eradication activities identify the attack and the compromised pathway, patch or clean the CDA, or replace the CDA using disaster recovery procedures. Measures necessary to mitigate the consequences of cyber attacks are as directed by site governing procedures.

Recovery activities include but are not limited to functional recovery test, cyber security function and requirements tests, restoration to operational state, verification of operability or functionality, and return to service. Systems, networks, and/or equipment affected by cyber attacks are restored and returned to operation as directed by site procedures. Post incident analysis is conducted in accordance with site Corrective Action Program procedures.

4.7 CYBER SECURITY CONTINGENCY PLAN

A Cyber Security Contingency Plan protects CDAs from adverse impacts from cyber attack. Refer to Appendix E of NEI 08-09, Revision 6, for additional Cyber Security Contingency Plan cyber security controls.

The contingency planning policy is developed, disseminated, periodically reviewed and updated. The contingency planning policy provides the following:

a. A formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organization entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the policy and associated contingency planning controls.

The Cyber Security Contingency Plan includes:

- Required response to events or conditions of varying duration and severity that would activate the recovery plan;
- Procedures for operating the CDAs in manual mode with external electronic communications connections severed until secure conditions can be restored;
- Roles and responsibilities of responders;
- Processes and procedures for the backup and secure storage of information;
- Complete and up-to-date logical diagrams depicting network connectivity;
- Current configuration information for components;

- Personnel list (according to title and/or function) for authorized physical and cyber access to the CDA;
- Communication procedure and list of personnel (according to title and/or function) to contact in the case of an emergency; and
- Documented requirements for the replacement of components.

4.8 CYBER SECURITY TRAINING AND AWARENESS

The Program establishes the training requirements necessary for licensee personnel and contractors to perform their assigned duties and responsibilities in implementing the requirements of the Program.

Individuals are trained to a level of cyber security knowledge commensurate with their assigned responsibilities in order to provide high assurance that individuals are able to perform their job functions. Refer to Appendix E of NEI 08-09, Revision 6, which describes the Cyber Security Controls required for the following levels of training:

- Awareness Training
- Technical Training
- Specialized Cyber Security Training

Specific topics included within the Cyber Security Training and Awareness program may be modified, added or deleted (1) in response to feedback from personnel and contractors who have taken the training, or (2) as a result of discussions with cyber security groups and associations.

4.9 EVALUATE AND MANAGE CYBER RISK

Cyber risk is evaluated and managed utilizing site programs and procedures.

4.9.1 Threat and Vulnerability Management

Cyber risks are managed through evaluation of threats and vulnerabilities to computer and control systems during the life cycle phases as documented in the Engineering Design Control, Configuration Management, Software Quality Assurance, Operating Experience and Corrective Action Program processes. The Program establishes in procedures or other plant documents how responses to threat notifications and vulnerabilities against a CDA received from a credible source are screened, evaluated and dispositioned.

4.9.2 Risk Mitigation

Protection and mitigation of cyber risk are achieved by applying cyber security controls to the CDAs within the scope of the Rule. Detailed information on how these requirements are implemented to achieve high assurance objectives of cyber security controls specified in this Plan is available on site for the NRC's inspections and audit.

4.9.3 Operational Experience

Operational Experience Program procedures establish how the operational experiences related to cyber security are screened to determine applicability, evaluated to determine significance, and dispositioned in an operational experience program. Any condition determined to be adverse as a result of the evaluation of operational experiences, is dispositioned in the Corrective Action Program.

4.9.4 Corrective Action Program

Corrective Action Program (CAP) procedures establish the criteria for adverse conditions and the requirements for corrective action. Adverse impact resulting from a cyber security condition is evaluated, tracked and dispositioned in accordance with the site Corrective Action Program.

4.10 POLICIES AND IMPLEMENTING PROCEDURES

Policies and implementing procedures are developed to meet the implemented cyber security control's objectives provided in Appendices D and E of NEI 08-09, Revision 6. The program policies and implementing procedures are documented, developed, reviewed, approved, issued, used, and revised as described in Section 4 of this Plan. Program policies and implementing procedures establish that personnel responsible for the management and implementation of the program report to senior nuclear management. Senior nuclear management is Vice President, Operations, who is accountable for nuclear plant(s) operation.

Implementing procedures establish responsibilities for the positions documented in Section 4.11.

4.11 ROLES AND RESPONSIBILITIES

Roles and responsibilities are implemented with site procedures to preclude conflict during both normal and emergency conditions. The following Roles are created and staffed with qualified and experienced personnel. Authorized contracted resources possessing the skill set identified below for their designated role may be used. Implementing procedures establish responsibilities for the following:

Cyber Security Program Sponsor

- Member of Senior Entergy Management;
- Overall responsibility and accountability for the cyber security program;
- Provide resources required for the development, implementation and sustenance of the cyber security program;
- Accountable to meet the needs of the site and receives support and compliance; and
- Ensure that resources are available to develop and implement the Program.

Cyber Security Program Manager

- The single point of contact accountable for any issues related to JAF cyber security;
- Responsible for oversight and assuring periodic assessments are performed in accordance with Section 4;
- Provides oversight of the plant cyber security operations;
- Functions as a single point of contact for issues related to cyber security;
- Provides oversight and direction on issues regarding nuclear plant cyber security;
- Initiates and coordinates CSIRT functions as required;
- Coordinates with NRC, Department of Homeland Security, Department of Energy, and Federal Bureau of Investigation as required during cyber security events;
- Oversees and approves the development and implementation of a Cyber Security Plan;
- Ensures and approves the development and operation of the cyber security education, awareness, and training program; and
- Oversees and approves the development and implementation of cyber security policies and procedures.

Cyber Security Specialists

- Protect CDAs from cyber threat;
- Understand the cyber security implications surrounding the overall architecture of plant networks, operating systems, hardware platforms, plant-specific applications, and the services and protocols upon which those applications rely;
- Perform cyber security assessments of CDAs;
- Conduct cyber security audits, network scans, and penetration tests against CDAs as necessary;
- Conduct cyber security investigations involving compromise of CDAs;
- Preserve evidence collected during cyber security investigations to prevent loss of evidentiary value;
- Maintain expert skill and knowledge level in the area of cyber security; and
- Receive specialized cyber security training described in Section 4.8.

CSIRT

- Initiates in accordance with the Incident Response Plan;
- Initiates emergency action when required to safeguard CDAs from cyber security compromise and to assist with the eventual recovery of compromised systems;
- Contains and mitigates incidents involving critical and other support systems;
- Restores compromised CDAs; and

- Responds to a cyber attack and performs the activities described in Section 4.6. Responsibilities are designated in site and Entergy incident response procedures. Ancillary CSIRT staff includes organizations and individuals who operate, maintain, or design critical systems. CSIRT support staff is comprised of organizations and individuals as needed for specific specialized knowledge.

Others

- Operators, engineers, technicians, and users perform their assigned duties in accordance with the requirements of the Program.

4.12 CYBER SECURITY PROGRAM REVIEW

The Cyber Security Program established the necessary measures and governing procedures to implement reviews of applicable program elements in accordance with the requirements of 10 CFR 73.55(m). Security Controls are elements of the Security Program and are reviewed consistent with the following requirements of 10 CFR 73.55(m).

(1) As a minimum the licensee shall review each element of the physical protection program at least every 24 months. Reviews shall be conducted:

  (i) Within 12 months following initial implementation of the physical protection program or a change to personnel, procedures, equipment, or facilities that potentially could adversely affect security.

  (ii) As necessary based upon site-specific analyses, assessments, or other performance indicators.

  (iii) By individuals independent of those personnel responsible for program management and any individual who has direct responsibility for implementing the onsite physical protection program.

(2) Reviews of the security program must include, but not be limited to, an audit of the effectiveness of the physical security program, security plans, implementing procedures, cyber security programs, safety/security interface activities, the testing, maintenance, and calibration program, and response commitments by local, State, and Federal law enforcement authorities.

(3) The results and recommendations of the onsite physical protection program reviews, management's findings regarding program effectiveness, and any actions taken as a result of recommendations from prior program reviews, must be documented in a report to the licensee's plant manager and to corporate management at least one level higher than that having responsibility for day-to-day plant operation. These reports must be maintained in an auditable form, available for inspection.

(4) Findings from onsite physical protection program reviews must be entered into the site corrective action program.

4.13 DOCUMENT CONTROL AND RECORDS RETENTION AND HANDLING

JAF 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 in accordance with policies/procedures 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.