

Joseph H. Plona
Site Vice President

6400 N. Dixie Highway, Newport, MI 48166
Tel: 734.586.5910 Fax: 734.586.4172

DTE Energy



Security-Related Information – Withhold Under 10 CFR 2.390

10 CFR 50.90

July 27, 2010
NRC-10-0050

U. S. Nuclear Regulatory Commission
Attention: Document Control Desk
Washington D C 20555-0001

- References:
- 1) Fermi 2
NRC Docket No. 50-341
NRC License No. NPF-43
 - 2) Detroit Edison's letter to the NRC, "Request for Approval of the Fermi 2 Cyber Security Plan," NRC-09-0063, dated November 19, 2009
 - 3) NRC Letter to Detroit Edison, "Fermi 2 – License Amendment Request for Approval of the Cyber Security Plan (TAC NO ME2678)," dated May 28, 2010

Subject: Request for Approval of Revised Fermi 2 Cyber Security Plan

In accordance with the provisions of 10 CFR 50.4 and 10 CFR 50.90, Detroit Edison is submitting this revised request for an amendment to the Facility Operating Licenses (FOL) for Fermi 2. This proposed amendment requests NRC approval of the revised Fermi 2 Cyber Security Plan, Implementation Schedule, and a FOL revision that adds a sentence to the existing Physical Protection license condition to require Fermi 2 to fully implement and maintain in effect all provisions of the Commission approved Cyber Security Plan. As requested in Reference 3, this letter withdraws the license amendment request submitted in Reference 2 and replaces it in its entirety with this request.

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

USNRC
NRC-10-0050
Page 2

In accordance with the alternative described in Reference 3, this proposed amendment is consistent with NEI 08-09, Revision 6, “Cyber Security Plan for Nuclear Power Reactors.”

Enclosure 1 provides an evaluation of the proposed change. Enclosure 2 provides the existing FOL page marked up to show the proposed revised change. Enclosure 3 provides the proposed FOL changes in final typed format. Enclosure 4 provides a copy of the Fermi 2 Cyber Security Plan revised proposed implementation schedule. Enclosure 5 provides a copy of the proposed revised Fermi 2 Cyber Security Plan. Enclosure 6 contains a list of deviations taken from NEI 08-09, Revision 6, Appendix A, Cyber Security Plan Template.

Detroit Edison requests that Enclosure 4, which contain security-related information, be withheld from public disclosure in accordance with 10 CFR 2.390.

In accordance with 10 CFR 50.91, a copy of this application, with attachments, is being provided to the designated Michigan State Official.

Detroit Edison requests an implementation period of 60 days following NRC approval of the license amendment.

Should you have any questions or require additional information, please contact Mr. Rodney W. Johnson of my staff at (734) 586-5076.

Sincerely,



Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

USNRC
NRC-10-0050
Page 3

- Enclosure 1 – Evaluation of the Proposed Change
- Enclosure 2 – Proposed Facility Operating License Change (Mark-Up)
- Enclosure 3 – Proposed Facility Operating License Change (Re-Typed)
- Enclosure 4 – Fermi 2 Cyber Security Plan Proposed Implementation Schedule
(Security-Related Information – Withhold Under 10 CFR 2.390)
- Enclosure 5 – Fermi 2 Cyber Security Plan
- Enclosure 6 – List Of Deviations Taken From NEI 08-09, Revision 6, Appendix A,
Cyber Security Plan Template

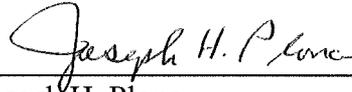
cc: NRC Project Manager
NRC Resident Office
Reactor Projects Chief, Branch 4, Region III
Regional Administrator, Region III
Supervisor, Electric Operators,
Michigan Public Service Commission (w/o Enclosure 4)

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

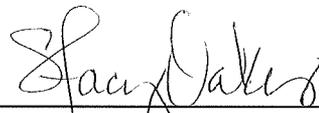
USNRC
NRC-10-0050
Page 4

I, Joseph H. Plona, do hereby affirm that the foregoing statements are based on facts and circumstances which are true and accurate to the best of my knowledge and belief.



Joseph H. Plona
Site Vice President, Nuclear Generation

On this 27th day of July, 2010 before me personally appeared Joseph H. Plona, being first duly sworn and says that he executed the foregoing as his free act and deed.



Notary Public

STACY OAKES
NOTARY PUBLIC, STATE OF MI
COUNTY OF MONROE
MY COMMISSION EXPIRES JUL 26, 2012
ACTING IN COUNTY OF MONROE, MI

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

**Enclosure 1
NRC-10-0050**

Evaluation of Proposed Change

Request for Approval of the Fermi 2 Cyber Security Plan

- 1.0 Summary Description
- 2.0 Detailed Description
- 3.0 Technical Evaluation
- 4.0 Regulatory Evaluation
 - 4.1 Applicable Regulatory Requirements / Criteria
 - 4.2 Significant Hazards Consideration
 - 4.3 Conclusion
- 5.0 Environmental Consideration
- 6.0 References

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 1 to
NRC-10-0050
Page 1

1.0 SUMMARY DESCRIPTION

This proposed license amendment request (LAR) includes the proposed Fermi 2 Cyber Security Plan (Plan), an Implementation Schedule, and a proposed sentence to be added to the existing Facility Operating License (FOL) Physical Protection license condition.

2.0 DETAILED DESCRIPTION

The proposed license amendment request (LAR) includes three parts: the proposed Plan, an Implementation Schedule, and a proposed sentence to be added to the existing FOL Physical Protection license condition to require Fermi 2 to fully implement and maintain in effect all provisions of the Commission approved cyber security plan as required by 10 CFR 73.54.

Federal Register notice 74 FR 13926 (Reference 1) issued the final rule that amended 10 CFR Part 73. The regulations in 10 CFR 73.54, "Protection of digital computer and communication systems and networks," establish the requirements for a cyber security program. This regulation specifically requires each licensee currently licensed to operate a nuclear power plant under Part 50 of this chapter to submit a cyber security plan that satisfies the requirements of the Rule. Each submittal must include a proposed implementation schedule and implementation of the licensee's cyber security program must be consistent with the approved schedule.

3.0 TECHNICAL EVALUATION

Reference 1 issued the final rule that amended 10 CFR Part 73. Cyber security requirements are codified as new 10 CFR 73.54 and are designed 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 established by 10 CFR 73.1(a)(1)(v). These requirements are substantial improvements upon the requirements imposed by NRC Order EA-02-026 (Reference 2).

This LAR includes the proposed Plan (Enclosure 5) that conforms to the template provided in NEI 08-09, Revision 6. In addition the LAR includes the proposed change to the existing FOL license condition for "Physical Protection" (Enclosures 2 and 3), a proposed Implementation Schedule (Enclosure 4) as required by 10 CFR 73.54, and a list of deviations from NEI 08-09, Revision 6 template (Enclosure 6).

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 1 to
NRC-10-0050
Page 2

4.0 REGULATORY EVALUATION

4.1 APPLICABLE REGULATORY REQUIREMENTS / CRITERIA

This LAR is submitted pursuant to 10 CFR 73.54 which requires licensees currently licensed to operate a nuclear power plant under 10 CFR Part 50 to submit a Cyber Security Plan in accordance with 10 CFR 50.4 and 10 CFR 50.90.

4.2 SIGNIFICANT HAZARDS CONSIDERATION

Detroit Edison has evaluated the proposed changes using the criteria in 10 CFR 50.92 and has determined that the proposed changes do not involve a significant hazards consideration. An analysis of the issue of no significant hazards consideration is presented below.

The proposed change incorporates a new requirement into the facility operating license to implement and maintain a cyber security plan. This new requirement is being included as part of an existing facility operating license condition that requires the implementation and maintenance of physical security, training and qualification, and safeguards contingency plans. The Cyber Security Plan describes how the requirements of 10 CFR 73.54 will be implemented in order to protect the health and safety of the public from radiological sabotage as a result of a cyber attack. The plan conforms to the template provided in NEI 08-09, Revision 6, with deviations, and provides a description of how the requirements of 10 CFR 73.54 will be implemented at Fermi 2.

The Cyber Security Plan establishes the licensing basis for the Cyber Security Program. The Cyber Security Plan establishes how to achieve high assurance that nuclear power plant digital computer and communication systems and networks associated with the following are adequately protected against cyber attacks up to and including the design basis threat:

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.

Criterion 1: The proposed change does not involve a significant increase in the probability or consequences of an accident previously evaluated.

The proposed change incorporates a new requirement, in the Operating License, to implement and maintain a cyber security plan as part of the facility's overall program for physical

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 1 to
NRC-10-0050
Page 3

protection. The Cyber Security Plan itself does not require any plant modifications. Rather, the Cyber Security Plan describes how the requirements of 10 CFR 73.54 are implemented in order to identify, evaluate, and mitigate cyber attacks up to and including the design basis threat, thereby achieving high assurance that the facility's digital computer and communications systems and networks are protected from cyber attacks. The proposed change requiring the implementation and maintenance of a Cyber Security Plan does not alter accident analysis assumptions, add any accident initiators, or affect the function of plant systems or the manner in which systems are operated.

Therefore, the inclusion of the Cyber Security Plan as a part of the facility's other physical protection programs specified in the facility's operating license has no impact on the probability or consequences of an accident previously evaluated.

Criterion 2: The proposed change does not create the possibility of a new or different kind of accident from any accident previously evaluated.

The proposed change incorporates a new requirement, in the Operating License, to implement and maintain a cyber security plan as part of the facility's overall program for physical protection. The creation of the possibility of a new or different kind of accident requires creating one or more new accident precursors. New accident precursors may be created by modifications of the plant's configuration, including changes in the allowable modes of operation. Issuance of the Cyber Security Plan itself does not require any modifications; however, implementation of the plan will require future modifications. The Cyber Security Plan does not affect the control parameters governing unit operation or the response of plant equipment to a transient condition. Because the proposed change does not change or introduce any new equipment, modes of system operation, or failure mechanisms, no new accident precursors are created.

Therefore, the proposed change does not create the possibility of a new or different kind of accident from any accident previously evaluated.

Criterion 3: The proposed change does not involve a significant reduction in a margin of safety.

The proposed change incorporates a new requirement, in the Operating License, to implement and maintain a cyber security plan as part of the facility's overall program for physical protection. Plant safety margins are established through Limiting Conditions for Operation, Limiting Safety System Settings, and Safety limits specified in the Technical Specifications. Because the Cyber Security Plan does not alter the operation of plant equipment, the proposed change does not change established safety margins. Therefore, the proposed change does not involve a significant reduction in a margin of safety.

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 1 to
NRC-10-0050
Page 4

4.3 CONCLUSION

In conclusion, based on the considerations discussed above: (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner; (2) such activities will be conducted in compliance with the Commission's regulations; and (3) the issuance of the amendment will not be inimical to the common defense and security or to the health and safety of the public.

5.0 ENVIRONMENTAL CONSIDERATION

The proposed amendment establishes the licensing basis for a Cyber Security Program for Fermi 2. This proposed amendment will not involve any significant construction impacts. Pursuant to 10 CFR 51.22(b)(12) no environmental impact statement or environmental assessment need be prepared in connection with the issuance of the amendment.

6.0 REFERENCES

1. Federal Register Notice, Final Rule 10 CFR Part 73, Power Reactor Security Requirements, published on March 27, 2009, 74 FR 13926.
2. EA-02-026, Order Modifying Licenses, Safeguards and Security Plan Requirements, issued February 25, 2002.

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

**Enclosure 2
NRC-10-0050**

Proposed Facility Operating License Change (Mark-Up)

Marked up page:

Operating License page 8

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

D. Exemptions from certain requirements of Appendices E and J to 10 CFR Part 50, are described in supplements to the SER. These include: (a) an exemption from the requirement of Section IV.F of Appendix E that a full participation emergency planning exercise be conducted within one year before issuance of the first operating license for full power and prior to operation above five percent of rated power (Section 13.3 of SSER #6); (b) an exemption from the requirement of Paragraph III.C.2(b) of Appendix J, the testing of the main steam isolation valves at the peak calculated containment pressure associated with the design basis accident (Section 6.2.7 of SSER #5); and (c) an exemption from the requirement of Paragraph III.D.2(b)(ii) of Appendix J, the testing of containment air locks at times when containment integrity is not required (Section 6.2.7 of SSER #5). These exemptions are authorized by law and will not endanger life or property or the common defense and security and are otherwise in the public interest. Therefore, these exemptions are hereby granted pursuant to 10 CFR 50.12. With the granting of these exemptions, the facility will operate, to the extent authorized herein, in conformity with the application, as amended, the provisions of the Act, and the rules and regulations of the Commission.

E. The licensee shall fully implement and maintain in effect all provisions of the Commission-approved physical security, training and qualification, and safeguards contingency plans including amendments made pursuant to provisions of the Miscellaneous Amendments and Search Requirements revisions to 10 CFR 73.55 (51 FR 27817 and 27822) and to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The plans, which contain Safeguards Information protected under 10 CFR 73.21, are entitled: "Fermi 2 Physical Security Plan, Security Training and Qualification Plan, and Safeguards Contingency Plan" submitted by letter dated September 9, 2004, and supplemented on October 7, 2004, and October 14, 2004, November 18, 2005, and May 18, 2006.

F. Deleted

↑
INSERT

G. The licensees shall have and maintain financial protection of such type and in such amounts as the Commission shall require in accordance with Section 170 of the Atomic Energy Act of 1954, as amended, to cover public liability claims.

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved Fermi 2 Cyber Security Plan.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 3

NRC-10-0050

Proposed Facility Operating License Change (Re-Typed)

Re-Typed page:

Operating License page 8

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

- D. Exemptions from certain requirements of Appendices E and J to 10 CFR Part 50, are described in supplements to the SER. These include: (a) an exemption from the requirement of Section IV.F of Appendix E that a full participation emergency planning exercise be conducted within one year before issuance of the first operating license for full power and prior to operation above five percent of rated power (Section 13.3 of SSER #6); (b) an exemption from the requirement of Paragraph III.C.2(b) of Appendix J, the testing of the main steam isolation valves at the peak calculated containment pressure associated with the design basis accident (Section 6.2.7 of SSER #5); and (c) an exemption from the requirement of Paragraph III.D.2(b)(ii) of Appendix J, the testing of containment air locks at times when containment integrity is not required (Section 6.2.7 of SSER #5). These exemptions are authorized by law and will not endanger life or property or the common defense and security and are otherwise in the public interest. Therefore, these exemptions are hereby granted pursuant to 10 CFR 50.12. With the granting of these exemptions, the facility will operate, to the extent authorized herein, in conformity with the application, as amended, the provisions of the Act, and the rules and regulations of the Commission.
- E. The licensee shall fully implement and maintain in effect all provisions of the Commission-approved physical security, training and qualification, and safeguards contingency plans including amendments made pursuant to provisions of the Miscellaneous Amendments and Search Requirements revisions to 10 CFR 73.55 (51 FR 27817 and 27822) and to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The plans, which contain Safeguards Information protected under 10 CFR 73.21, are entitled: "Fermi 2 Physical Security Plan, Security Training and Qualification Plan, and Safeguards Contingency Plan" submitted by letter dated September 9, 2004, and supplemented on October 7, 2004, and October 14, 2004, November 18, 2005, and May 18, 2006. The licensee shall fully implement and maintain in effect all provisions of the Commission-approved Fermi 2 Cyber Security Plan.
- F. Deleted
- G. The licensees shall have and maintain financial protection of such type and in such amounts as the Commission shall require in accordance with Section 170 of the Atomic Energy Act of 1954, as amended, to cover public liability claims.

Security-Related Information – Withhold Under 10 CFR 2.390

**Enclosure 4
NRC-10-0050**

Fermi 2 Cyber Security Plan Proposed Implementation Schedule

Security-Related Information – Withhold Under 10 CFR 2.390

**Enclosure 5
NRC-10-0050**

Fermi 2 Cyber Security Plan

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 1

FERMI 2 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 Fermi 2. 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. Detroit Edison 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 Fermi 2.

A Glossary of terms used within this Plan and Appendices of 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 SSEP functions.

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 2

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 RG 5.69, “Guidance for the Application of the Radiological Sabotage Design Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements.” (Safeguards Information (SGI))

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)).

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 3

- 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 design basis threat of radiological sabotage as stated in 10 CFR73.1 at all times. (10 CFR 73.54(e)(2)(i), 10 CFR 73.54(e)(2)(iv) and 10 CFR73.55(b)(2)).
- 2.2.14 Maintain the capability to correct exploited vulnerabilities. (10 CFR73.54(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)).

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 4

- 2.2.18 Coordinate implementation of this Plan and associated procedures with other Fermi 2 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 Fermi 2 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

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 5

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

Fermi 2 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.

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 6

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.

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 7

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.

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 8

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 (HVAC); 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:

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 9

- 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.

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 10

- 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:

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 11

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; and
 - c. Implementing alternative countermeasures that provide at least the same degree of cyber security protection as the corresponding cyber security control;
 - 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., NIST, IEEE, ISO)
 - vii. Audits and Assessments
 - viii. Benchmarking
 - ix. Availability of new technologies.
3. Not implementing one or more of the cyber security controls by:

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 12

- 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.

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 13

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 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 within Section 4 of this Plan.

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 14

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 4 layers, with layer 4 having the greatest level of protection.
- Safety and important to safety CDAs are in Level 4.
- Security CDAs are in Levels 4 and 3.
- The boundary between Level 3 and Level 2 is implemented by one or more deterministic devices (i.e., data diodes, air gaps) that isolate CDAs in or above Level 3. Information flows between Level 4 and 3 are restricted through the use of one or more deterministic devices (i.e., data diodes, air gaps) that isolate CDAs or a firewall and network based intrusion detection system. The firewall implements the Information Flow Enforcement cyber security control in NEI 08-09, Revision 6, Appendix D, Section 1.4 and the rule set characteristics for non-deterministic information flow enforcement described in the Defense-In-Depth cyber security control in NEI 08-09, Revision 6, Appendix E, Section 6.

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:

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 15

- 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 and Configuration Management procedures, so that additional cyber security risk is not introduced into the system. The process ensures that

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 16

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.

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 17

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 continuing 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:

- 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

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 18

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 process 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 Design Basis Threat.

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.

Procedures have been established, implemented, and maintained to control life cycle phase activity cyber security controls for CDAs. These 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.

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 19

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

Policies and 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. 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 appropriate Operations, Security, and Information Technology personnel and require activation of Cyber Security Incident Response Team. 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;

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 20

- Isolate the affected CDA with approval by the Operations Shift Manager, 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;

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 21

- 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

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 22

Experience (OE) and Corrective Action Program (CAP) processes. The Program establishes in procedures 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

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

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 directly or indirectly to senior nuclear management. Senior nuclear management is the Site Vice-President 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:

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 23

Cyber Security Program Sponsor

- Member of Senior Fermi 2 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 Fermi 2 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 Cyber Security Incident Response Team (CSIRT) functions as required;
- Coordinates with NRC, DHS, DOE, and FBI 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.

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 24

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.

Cyber Security Incident Response Team (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 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.

<p>Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.</p>

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 25

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.

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 26

4.13 Document Control And Records Retention And Handling

Fermi 2 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

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 5 to
NRC-10-0050
Page 27

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.

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

**Enclosure 6
NRC-10-0050**

List Of Deviations Taken From NEI 08-09, Revision 6

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.

Security-Related Information – Withhold Under 10 CFR 2.390

Enclosure 6
NRC-10-0050
Page 1

List Of Deviations Taken From NEI 08-09, Revision 6

Deviation Number	NEI 08-09 Location	NEI 08-09, Revision 6 Text	Fermi 2 Cyber Security Plan Text	Justification
1	Appendix B, Cyber Attack Definition	<p>Any event in which there is reason to believe that an adversary has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause malicious exploitation of a SSEP function.</p> <p>[Note: Derived from the following sources: 10CFR 73.71(b); 10CFR 73 Appendix G; DG-5019, 10CFR 73.55(f); 72 FR 12723, 12724]</p>	<p>Any event in which there is reason to believe that an adversary has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause malicious exploitation of a CDA.</p>	<p>Revised per letter from Christopher E. Earls (NEI) to Richard P. Correia (USNRC), "NEI 08-09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors," April 2010," dated June 2, 2010.</p>

Enclosure 4 contains Security Related Information – Withhold Under 10 CFR 2.390. Upon Separation from Enclosure 4, the cover letter and other Enclosures are DECONTROLLED.