Entergy

Entergy Operations, Inc.
P.O. Box 756
Port Gibson, MS 39150
Tel 601 437 2800

GNRO-2009/00059

November 18, 2009

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

SUBJECT: Operating License Amendment Request
Grand Gulf Nuclear Station Cyber Security Plan and Implementation Schedule

Grand Gulf Nuclear Station, Unit 1
Docket No. 50-416
License No. NPF-29

Dear Sir or Madam:

In accordance with the provisions of 10 CFR 50.90, Entergy Operations, Inc. (Entergy) is submitting a request for an amendment to the Facility Operating License (FOL) for Grand Gulf Nuclear Station, Unit 1 (GGNS). The proposed amendment adds a sentence to the existing FOL Physical Protection license condition to require Entergy to fully implement and maintain in effect all provisions of the Commission-approved cyber security plan. Additionally, Entergy requests NRC approval of the GGNS Cyber Security Plan and associated implementation schedule in accordance with 10 CFR 73.54.

This proposed amendment generally conforms to the model Cyber Security Plan contained in Appendix A, "Cyber Security Plan Template", of NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors", Revision 3, September 2009.

Attachment 1 provides an analysis of the proposed FOL change for the GGNS Cyber Security Plan. Attachment 2 provides the existing FOL page marked-up to show the proposed change, and Attachment 3 provides the final typed FOL page. Attachment 4 provides a proposed implementation schedule. Attachment 5 identifies GGNS Cyber Security Plan deviations from NEI 08-09 Appendix A, Revision 3. Attachment 6 provides a copy of the GGNS Cyber Security Plan which is a standalone document to be incorporated by reference into the GGNS Physical Security Plan upon NRC approval. Entergy requests that Attachments 5 and 6, which contain security sensitive information, be withheld from public disclosure in accordance with 10 CFR 2.390.

The proposed change has been evaluated in accordance with 10 CFR 50.91(a)(1) using criteria in 10 CFR 50.92(c), and it has been determined that this change involves no significant hazards consideration. The bases for these determinations are included in Attachment 1.

Attachments 5 and 6 to this letter contain security sensitive information and are withheld from public disclosure in accordance with 10 CFR 2.390

S001

The list of new commitments is provided in Attachment 4.

Entergy requests approval of the proposed amendment, and the GGNS Cyber Security Plan and associated implementation schedule as soon as practical. Although this request is neither exigent nor emergency, your prompt review is requested. Once approved, the amendment will be implemented within 60 days of receipt of the approval letter. The implementation of the GGNS Cyber Security Plan will be in accordance with the approved schedule (Attachment 4).

If you have any questions regarding this submittal, please contact Peggy R. Rescheske at 601-437-1781.

I declare under penalty of perjury that the foregoing is true and correct. Executed on November 18, 2009.

Sincerely,

Christina L. Perino
Acting - Director, Nuclear Safety Assurance

CLP/PRR

Attachments:

1. Analysis of Proposed Operating License Change - GGNS Cyber Security Plan
2. Proposed GGNS Operating License Change (markup)
3. Proposed GGNS Operating License Change (typed final)
4. GGNS Cyber Security Plan Proposed Implementation Schedule - List of Regulatory Commitments
5. GGNS Cyber Security Plan Deviations from Appendix A of NEI 08-09 Revision 3 [Security-Related Information - Withhold from public disclosure under 10 CFR 2.390]
6. GGNS Cyber Security Plan [Security-Related Information - Withhold from public disclosure under 10 CFR 2.390]

cc:

NRC Senior Resident Inspector
Grand Gulf Nuclear Station
Port Gibson, MS 39150

U.S. Nuclear Regulatory Commission
ATTN: Mr. Elmo E. Collins, Jr. (w/2)
Region Administrator, Region IV
612 East Lamar Blvd, Suite 400
Arlington, TX 76011-4005

U. S. Nuclear Regulatory Commission
ATTN: Mr. Carl F. Lyon, NRR/ADRO/DORL (w/2)
Mail Stop OWFN/8 B1
Washington, DC 20555-0001

Attachment 1

GNRO-2009/00059

Analysis of Proposed Operating License Change -
GGNS Cyber Security Plan

1.0 Summary Description

The proposed license amendment request (LAR) adds a sentence to the existing Facility Operating License (FOL) Physical Protection license condition requiring Entergy Operations, Inc. (Entergy) to fully implement and maintain in effect all provisions of the Commission-approved cyber security plan. This submittal also includes the proposed Grand Gulf Nuclear Station, Unit 1 (GGNS) Cyber Security Plan (Plan) and an implementation schedule.

2.0 Detailed Description

The proposed change 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 the licensee to fully implement and maintain in effect all provisions of the Commission approved cyber security plan as required by 10 CFR 73.54 (Rule). Federal Register Notice 74 FR 13926, dated March 27, 2009, 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. The background for this application is addressed by the NRC Notice of Availability published on March 27, 2009, in Federal Register Notice 74 FR 13926 (Reference 1).

3.0 Technical Evaluation

Federal Register Notice 74 FR 13926 issued the final rule that amended 10 CFR Part 73. Cyber security requirements are codified in the 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).

NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 3, September 2009 (Reference 3) was used by licensees in development of their cyber security plans. Revision 3 of NEI 08-09 is a result of NEI/industry efforts and discussions with NRC. Deviations taken from Revision 3 of NEI 08-09 reflect subsequent industry discussions with the NRC.

This LAR includes the proposed Plan (Attachment 6) that generally conforms to the model Cyber Security Plan contained in Appendix A, "Cyber Security Plan Template", of NEI 08-09 Revision 3. Attachment 5 identifies deviations from the plan template in NEI 08-09 Appendix A, Revision 3. Deviations from the guidance in NEI 08-09, Appendices D and E, Revision 3, are included in the proposed Plan (Attachment 6). In addition, the LAR includes the proposed change to the existing FOL license condition for "Physical Protection" (Attachments 2 and 3). The LAR also contains the proposed implementation schedule (Attachment 4) as required by 10 CFR 73.54.

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 as specified in 10 CFR 50.4 and 10 CFR 50.90.

4.2 Significant Hazards Consideration

Entergy Operations, Inc. (Entergy) 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.

Criterion 1: The proposed change does not involve a significant increase in the probability or consequences of an accident previously evaluated.
The proposed change is required by 10 CFR 73.54 and includes three parts. The first part is the submittal of the Grand Gulf Nuclear Station, Unit 1 (GGNS) Cyber Security Plan (Plan) for NRC review and approval. The Plan generally conforms to the template provided in NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 3, September 2009, and provides a description of how the requirements of the Rule will be implemented at GGNS. The Plan establishes the licensing basis for the Cyber Security Program for GGNS. The 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.

Part one of the proposed change is designed to achieve high assurance that the systems within the scope of the Rule are protected from cyber attacks. The Plan itself does not require any plant modifications. However, the Plan does describe how plant modifications which involve digital computer systems are reviewed to provide high assurance of adequate protection against cyber attacks, up to and including the design basis threat as defined in the Rule. The proposed change does not alter the plant configuration, require new plant equipment to be installed, alter accident analysis assumptions, add any initiators, or affect the function of plant systems or the manner in which systems are operated, maintained, modified, tested, or inspected. The first part of the proposed change is designed to achieve high assurance that the systems within the scope of the Rule are protected from cyber attacks and has no impact on the probability or consequences of an accident previously evaluated.

The second part of the proposed change is an implementation schedule. The third part adds a sentence to the existing Facility Operating License (FOL) license condition for Physical Protection. Both of these changes are administrative and have no impact on the probability or consequences of an accident previously evaluated.

Therefore, it is concluded that the proposed change does not involve a significant increase in 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 is required by 10 CFR 73.54 and includes three parts. The first part is the submittal of the Plan for NRC review and approval. The Plan generally conforms to the template provided by NEI 08-09 and provides a description of how the requirements of the Rule will be implemented at GGNS. The Plan establishes the licensing basis for the Cyber Security Program for GGNS. The 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.

Part one of the proposed change is designed to achieve high assurance that the systems within the scope of the Rule are protected from cyber attacks. The Plan itself does not require any plant modifications. However, the Plan does describe how plant modifications involving digital computer systems are reviewed to provide high assurance of adequate protection against cyber attacks, up to and including the design basis threat defined in the Rule. The proposed change does not alter the plant configuration, require new plant equipment to be installed, alter accident analysis assumptions, add any initiators, or affect the function of plant systems or the manner in which systems are operated, maintained, modified, tested, or inspected. The first part of the proposed change is designed to achieve high assurance that the systems within the scope of the Rule are protected from cyber attacks and does not create the possibility of a new or different kind of accident from any previously evaluated.

The second part of the proposed change is an implementation schedule. The third part adds a sentence to the existing FOL license condition for Physical Protection. Both of these changes are administrative and do not create the possibility of a new or different kind of accident from any previously evaluated.

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

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

The proposed change is required by 10 CFR 73.54 and includes three parts. The first part is the submittal of the Plan for NRC review and approval. The Plan generally conforms to the template provided by NEI 08-09 and provides a description of how the requirements of the Rule will be implemented at GGNS. The Plan establishes the licensing basis for the Cyber Security Program for GGNS. The 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.

Part one of the proposed change is designed to achieve high assurance that the systems within the scope of the Rule are protected from cyber attacks. Plant safety margins are established through Limiting Conditions for Operation, Limiting Safety System Settings, and Safety Limits specified in the Technical Specifications. Because there is no change to these established safety margins, the proposed change does not involve a significant reduction in a margin of safety.

The second part of the proposed change is an implementation schedule. The third part adds a sentence to the existing FOL license condition for Physical Protection. Both of these changes are administrative and do not involve a significant reduction in a margin of safety.

Therefore, it is concluded that the proposed change does not involve a significant reduction in a margin of safety.

Based on the above, Entergy concludes that the proposed change presents no significant hazards consideration under the standards set forth in 10 CFR 50.92(c), and accordingly, a finding of no significant hazards consideration is justified.

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 GGNS and will be incorporated by reference into the Physical Security Plan. This proposed amendment will not involve any significant construction impacts. The proposed amendment meets the eligibility criterion for a categorical exclusion set forth in 10 CFR 51.22(c)(12). Therefore, pursuant to 10CFR51.22(b), Entergy concludes 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. NRC Order EA-02-026, Order Modifying Licenses, Safeguards and Security Plan Requirements, issued February 25, 2002
3. Nuclear Energy Institute NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 3, September 2009

Attachment 2

GNRO-2009/00059

Proposed GGNS Operating License Change (markup)

(b) The first performance of the periodic assessment of CRE habitability, Specification 5.5.13.c.(ii), shall be within 3 years, plus the 9-month allowance of SR 3.0.2, as measured from March 2005, the date of the most recent successful tracer gas test, as stated in the June 30, 2005 letter response to Generic Letter 2003-01, or within the next 9 months if the time period since the most recent successful tracer gas test is greater than 3 years.

(c) The first performance of the periodic assessment of the CRE boundary, Specification 5.5.13.d, shall be within the next 18 months, plus the 136 days allowed by SR 3.0.2, as measured from the date of issuance of this amendment.

D. The facility required exemptions from certain requirements of Appendices A and J to 10 CFR Part 50 and from certain requirements of 10 CFR Part 100. These include: (a) exemption from General Design Criterion 17 of Appendix A until startup following the first refueling outage, for (1) the emergency override of the test mode for the Division 3 diesel engine, (2) the second level undervoltage protection for the Division 3 diesel engine, and (3) the generator ground over current trip function for the Division 1 and 2 diesel generators (Section 8.3.1 of SSER #7) and (b) exemption from the requirements of Paragraph III.D.2(b)(ii) of Appendix J for the containment airlock testing following normal door opening when containment integrity is not required (Section 6.2.6 of SSER #7). 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. In addition, by exemption dated December 20, 1986, the Commission exempted licensees from 10 CFR 100.11(a)(1), insofar as it incorporates the definition of exclusion area in 10 CFR 100.3(a), until April 30, 1987 regarding demonstration of authority to control all activities within the exclusion area (safety evaluation accompanying Amendment No. 27 to License (NPF-29). This exemption is authorized by law, and will not present an undue risk to the public health and safety, and is consistent with the common defense and security. In addition, special circumstances have been found justifying the exemption. 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 provision 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: "Physical Security, Safeguards Contingency and Training and Qualification Plan," and were submitted to the NRC on May 18, 2006.

INSERT → The licensee shall fully implement in accordance with an NRC-approved implementation schedule and maintain in effect all provisions of the Commission-approved cyber security plan submitted by letter dated November 18, 2009, and withheld from public disclosure in accordance with 10 CFR 2.390.

Attachment 3

GNRO-2009/00059

Proposed GGNS Operating License Change (typed final)

(b) The first performance of the periodic assessment of CRE habitability, Specification 5.5.13.c.(ii), shall be within 3 years, plus the 9-month allowance of SR 3.0.2, as measured from March 2005, the date of the most recent successful tracer gas test, as stated in the June 30, 2005 letter response to Generic Letter 2003-01, or within the next 9 months if the time period since the most recent successful tracer gas test is greater than 3 years.

(c) The first performance of the periodic assessment of the CRE boundary, Specification 5.5.13.d, shall be within the next 18 months, plus the 136 days allowed by SR 3.0.2, as measured from the date of issuance of this amendment.

D. The facility required exemptions from certain requirements of Appendices A and J to 10 CFR Part 50 and from certain requirements of 10 CFR Part 100. These include: (a) exemption from General Design Criterion 17 of Appendix A until startup following the first refueling outage, for (1) the emergency override of the test mode for the Division 3 diesel engine, (2) the second level undervoltage protection for the Division 3 diesel engine, and (3) the generator ground over current trip function for the Division 1 and 2 diesel generators (Section 8.3.1 of SSER #7) and (b) exemption from the requirements of Paragraph III.D.2(b)(ii) of Appendix J for the containment airlock testing following normal door opening when containment integrity is not required (Section 6.2.6 of SSER #7). 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. In addition, by exemption dated December 20, 1986, the Commission exempted licensees from 10 CFR 100.11(a)(1), insofar as it incorporates the definition of exclusion area in 10 CFR 100.3(a), until April 30, 1987 regarding demonstration of authority to control all activities within the exclusion area (safety evaluation accompanying Amendment No. 27 to License (NPF-29). This exemption is authorized by law, and will not present an undue risk to the public health and safety, and is consistent with the common defense and security. In addition, special circumstances have been found justifying the exemption. 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 provision 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: "Physical Security, Safeguards Contingency and Training and Qualification Plan," and were submitted to the NRC on May 18, 2006.

The licensee shall fully implement in accordance with an NRC-approved implementation schedule and maintain in effect all provisions of the Commission-approved cyber security plan submitted by letter dated November 18, 2009, and withheld from public disclosure in accordance with 10 CFR 2.390.

Attachment 4

GNRO-2009/00059

GGNS Cyber Security Plan Proposed Implementation Schedule - List of Regulatory Commitments

GGNS Cyber Security Plan Proposed Implementation Schedule
List of Regulatory Commitments

The table below identifies the proposed implementation schedule and corresponding actions discussed in this letter for which Entergy commits to perform. Any other statements or actions discussed in this submittal are for information purposes and are not considered commitments.

COMMITMENT	TYPE		SCHEDULED COMPLETION DATE (If Required)
	ONE-TIME ACTION	CONTINUING COMPLIANCE	
1. The Cyber Security Program will be incorporated by reference into the Physical Protection Program.	X		Within 60 days following NRC approval of license amendment
2. The analysis of digital computer systems and networks in accordance with Chapter 3 of the Cyber Security Plan will be performed and results documented.	X		Within 36 months following NRC approval of license amendment
3. For cyber security controls that have been identified for implementation by the process described in Chapter 3 of the Cyber Security Plan, an implementation plan will be prepared and available for NRC inspection.	X		Within 48 months following NRC approval of license amendment
4. The elements to establish, implement, and maintain the Cyber Security Program as described in Chapter 4 of the Cyber Security Plan will be implemented.		X	Within 60 months following NRC approval of license amendment