



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

May 25, 2016

Vice President, Operations
Entergy Operations, Inc.
Grand Gulf Nuclear Station
P.O. Box 756
Port Gibson, MS 39150

SUBJECT: GRAND GULF NUCLEAR STATION, UNIT 1 - ISSUANCE OF AMENDMENT
RE: CYBER SECURITY PLAN MILESTONE 8 FULL IMPLEMENTATION
SCHEDULE (CAC NO. MF6566)

Dear Sir or Madam:

The U.S. Nuclear Regulatory Commission has issued the enclosed Amendment No. 210 to Facility Operating License No. NPF-29 for the Grand Gulf Nuclear Station, Unit 1 (GGNS). This amendment consists of changes to the facility operating license in response to your application dated June 29, 2015.

The amendment approves a change to the GGNS facility operating license to revise the Cyber Security Plan (CSP) Milestone 8 full implementation date from June 30, 2016 to December 15, 2017, as set forth in the CSP Implementation Schedule.

A copy of the related Safety Evaluation is enclosed. The Notice of Issuance will be included in the Commission's next biweekly *Federal Register* notice.

Sincerely,

A handwritten signature in cursive script that reads "James Kim".

James Kim, Project Manager
Plant Licensing IV-2 and Decommissioning
Transition Branch
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-416

Enclosures:

1. Amendment No. 210 to NPF-29
2. Safety Evaluation

cc w/encls: Distribution via Listserv



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

ENERGY OPERATIONS, INC.
SYSTEM ENERGY RESOURCES, INC.
SOUTH MISSISSIPPI ELECTRIC POWER ASSOCIATION
ENERGY MISSISSIPPI, INC.
DOCKET NO. 50-416
GRAND GULF NUCLEAR STATION, UNIT 1
AMENDMENT TO FACILITY OPERATING LICENSE

Amendment No. 210
License No. NPF-29

1. The Nuclear Regulatory Commission (the Commission) has found that:
 - A. The application for amendment by Entergy Operations, Inc. (the licensee), dated June 29, 2015, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act), and the Commission's rules and regulations set forth in 10 CFR Chapter I;
 - B. The facility will operate in conformity with the application, the provisions of the Act, and the rules and regulations of the Commission;
 - C. There is reasonable assurance (i) that the activities authorized by this amendment can be conducted without endangering the health and safety of the public, and (ii) that such activities will be conducted in compliance with the Commission's regulations;
 - D. The issuance of this amendment will not be inimical to the common defense and security or to the health and safety of the public; and
 - E. The issuance of this amendment is in accordance with 10 CFR Part 51 of the Commission's regulations and all applicable requirements have been satisfied.

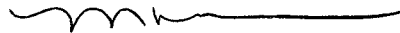
Enclosure 1

2. Accordingly, the license is amended as indicated in the attachment to this license amendment, and paragraph 2.E of Facility Operating License No. NPF-29 is hereby amended to read, in part, as follows:

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The licensee's CSP was approved by License Amendment No. 186 as supplemented by a change approved by License Amendment Nos. 192, 200, and 210.

3. This license amendment is effective as of its date of issuance and shall be implemented within 30 days from the date of issuance. The full implementation of the CSP shall be in accordance with the implementation schedule submitted by the licensee on June 29, 2015, and approved by the NRC staff with this license amendment. All subsequent changes to the NRC-approved CSP implementation schedule will require NRC approval pursuant to 10 CFR 50.90.

FOR THE NUCLEAR REGULATORY COMMISSION



Meena K. Khanna, Chief
Plant Licensing IV-2 and Decommissioning
Transition Branch
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to the Facility Operating
License No. NPF-29

Date of Issuance: May 25, 2016

ATTACHMENT TO LICENSE AMENDMENT NO. 210

FACILITY OPERATING LICENSE NO. NPF-29

DOCKET NO. 50-416

Replace the following page of the Facility Operating License No. NPF-29 with the attached revised page. The revised page is identified by amendment number and contains a marginal line indicating the area of change.

Facility Operating License

REMOVE

16g

INSERT

16g

- 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 and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The licensee's CSP was approved by License Amendment No. 186 as supplemented by a change approved by License Amendment Nos. 192, 200, and 210.



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 210 TO

FACILITY OPERATING LICENSE NO. NPF-29

ENTERGY OPERATIONS, INC., ET AL.0

GRAND GULF NUCLEAR STATION, UNIT 1

DOCKET NO. 50-416

1.0 INTRODUCTION

By application dated June 29, 2015 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML15180A376), Entergy Operations Inc. (Entergy, the licensee), requested a change to the facility operating license (FOL) for Grand Gulf Nuclear Station, Unit 1 (GGNS). The proposed change would revise the date of Cyber Security Plan (CSP) Implementation Schedule Milestone 8 and the existing license condition in the FOL. Milestone 8 of the CSP implementation schedule concerns the full implementation of the CSP.

The U.S. Nuclear Regulatory Commission (NRC) staff initially reviewed and approved the licensee's original CSP implementation schedule for GGNS by Amendment No. 186, dated July 27, 2011 (ADAMS Accession No. ML111940165). Subsequently, the NRC staff reviewed and approved Amendment No. 200, dated December 12, 2014, which extended the CSP implementation schedule (ADAMS Accession No. ML14311A479). This schedule required GGNS to fully implement and maintain all provisions of the CSP no later than June 30, 2016.

The proposed change would revise the completion date of the CSP Implementation Schedule Milestone 8 and paragraph 2.E in the FOL from June 30, 2016 to December 15, 2017. Milestone 8 of the CSP implementation schedule and paragraph 2.E concern the full implementation of the CSP. The NRC issued a proposed finding that the amendment involves no significant hazards consideration, published in the *Federal Register* on October 13, 2015 (80 FR 61481). The NRC has not received public comment on this determination.

2.0 REGULATORY EVALUATION

The NRC staff considered the following regulatory requirements and guidance in its review of the current license amendment request to modify the existing CSP implementation schedule:

- Title 10 of the *Code of Federal Regulations* (10 CFR) Section 73.54, "Protection of digital computer and communication systems and networks," which states, in part: "Each [CSP] submittal must include a proposed implementation schedule. Implementation of the licensee's cyber security program must be consistent with the approved schedule."
- The licensee's FOL includes a license condition that requires the licensee to fully implement and maintain in effect all provisions of the Commission-approved CSP.
- NRC Memorandum, "Review Criteria for Title 10 of the *Code of Federal Regulations* Part 73.54, Cyber Security Implementation Schedule Milestone 8 License Amendment Requests," dated October 24, 2013 (ADAMS Accession No. ML13295A467), in which the NRC staff lists criteria to consider during evaluations of licensees' requests to postpone their cyber security program implementation date (commonly known as Milestone 8).

The NRC staff does not regard the CSP milestone implementation dates as regulatory commitments that can be changed unilaterally by the licensee, particularly in light of the regulatory requirement at 10 CFR 73.54, that states, "[i]mplementation of the licensee's cyber security program must be consistent with the approved schedule." As the NRC staff explained in its letter to all operating reactor licensees dated May 9, 2011 (ADAMS Accession No. ML110980538), the implementation of the plan, including the key intermediate milestone dates and the full implementation date shall be in accordance with the implementation schedule submitted by the licensee and approved by the NRC. All subsequent changes to the NRC-approved CSP implementation schedule, thus, will require prior NRC approval pursuant in 10 CFR 50.90, "Application for amendment of license, construction permit, or early site permit."

3.0 TECHNICAL EVALUATION

3.1 Licensee's Requested Change

The NRC staff issued Amendment No. 200 to FOL No. NPF-29 for GGNS by letter dated December 12, 2014. The NRC staff approved the licensee's CSP implementation schedule, as discussed in the safety evaluation issued with the amendment. The licensee's implementation schedule was based on a template prepared by the Nuclear Energy Institute (NEI), which was transmitted to the NRC by letter dated February 28, 2011 (ADAMS Accession No. ML11060206). By letter dated March 1, 2011, the NRC staff found the NEI template acceptable for licensees to use to develop their CSP implementation schedules (ADAMS Accession No. ML110073048). The licensee's proposed implementation schedule for the CSP identified completion dates and bases for the following eight milestones:

- 1) Establish the Cyber Security Assessment Team (CSAT);
- 2) Identify Critical Systems (CSs) and Critical Digital Assets (CDAs);
- 3) Install a deterministic one-way devices between lower level devices and higher level devices;

- 4) Implement the security control "Access Control For Portable And Mobile Devices";
- 5) Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds by incorporating the appropriate elements;
- 6) Identify, document, and implement technical cyber security controls in accordance with "Mitigation of Vulnerabilities and Application of Cyber Security Controls" for CDAs that could adversely impact the design function of physical security target set equipment;
- 7) Ongoing monitoring and assessment activities for those target set CDAs whose security controls have been implemented; and
- 8) Fully implement the CSP.

Currently, Milestone 8 of the GGNS CSP requires the licensee to fully implement the CSP by June 30, 2016. In its application dated June 29, 2015, Entergy proposed to change the Milestone 8 completion date to December 15, 2017.

The licensee submitted its application on June 29, 2015, using the NRC staff's guidance to evaluate requests to postpone Milestone 8 implementation dates. The licensee's application addressed all the criteria in the guidance. The intent of the staggered cyber security implementation schedule was for licensees to demonstrate ongoing implementation of their cyber security program prior to full implementation, which was scheduled for the date specified in Milestone 8. The licensee completed seven other milestones (Milestone 1 through Milestone 7) by December 31, 2012. Activities included establishing a CSAT, identifying CSs and CDAs, installing deterministic one-way devices between defensive levels, implementing access control for portable and mobile devices, implementing methods to observe and identify obvious cyber related tampering, and conducting ongoing monitoring and assessment activities for target set CDAs. In their aggregate, the interim milestones demonstrate ongoing implementation of the cyber security program.

The licensee provided the following information pertinent to each of the criteria identified in the NRC guidance memorandum, dated October 24, 2013, as summarized below.

- 1) Identification of the specific requirement or requirements of the cyber security plan that the licensee needs additional time to implement.

The licensee stated that the following requirements of the CSP require additional time to implement: Section 3, "Analyzing Digital Computer Systems and Networks," and Section 4, "Establishing, Implementing and Maintaining the Cyber Security Program." The licensee further noted that these sections describe the process for application and maintenance of cyber security controls and the process of addressing security controls. Also, the licensee noted any combination of physical, logical (software-related), or programmatic/procedural changes could be required.

- 2) Detailed justification that describes the reason the licensee requires additional time to implement the specific requirement or requirements identified.

The licensee stated that Entergy hosted a "pilot" Milestone 8 inspection at the Indian Point site in March 2014. During the pilot, insight was gained into the NRC perspective on how to apply the cyber security controls listed in NEI 08-09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors," dated April 2010 (ADAMS Accession No. ML101180437). During the pilot inspection, the NRC team reviewed several examples of CDAs with Entergy and indicated the level of detail and depth expected for the technical analyses against cyber security controls referenced in NEI 08-09. Based on this review, Entergy stated that the detail and depth of the technical analysis exceeds Entergy's prior understanding and necessitates a greater effort to achieve than initially anticipated.

The licensee stated that during 2015, an inspection of compliance associated with interim Milestones 1 through 7 for each operating Entergy licensee. The preparation for and support of these inspections required a significant commitment of time from Entergy's most knowledgeable subject matter experts on nuclear cyber security, exceeding the estimate previously developed and therefore, drawing those resources away from Milestone 8 implementation activities.

- 3) A proposed completion date for Milestone 8 consistent with the remaining scope of work to be conducted and the resources available.

The licensee proposed a Milestone 8 completion date of December 15, 2017.

- 4) An evaluation of the impact that the additional time to implement the requirements will have on the effectiveness of the licensee's overall cyber security program in the context of milestones already completed.

The licensee indicated the impact of the requested additional implementation time on the effectiveness of the overall cyber security program is very low. The milestones already completed have resulted in a high degree of protection of safety-related, important-to-safety, and security CDAs against common threat vectors. Additionally, the licensee stated that extensive physical and administrative measures are already in place for CDAs because they are plant components, pursuant to the Physical Security Plan and Technical Specification requirements. The licensee also briefly described how it had implemented the various milestones.

- 5) A description of the licensee's methodology for prioritizing completion of work for CDAs associated with significant safety, security or emergency preparedness (SSEP) consequences and with reactivity effects in the balance-of-plant (BOP).

The licensee stated that because CDAs are plant components, prioritization follows the normal work management process that places the highest priority on apparent conditions adverse to quality in system, structure, and component design function and related factors such as safety risk and nuclear defense-in-depth, as well as threats to continuity of electric power generation in the BOP. High focus continues to be maintained on prompt attention to any emergent issue with these CDAs that would potentially challenge the established cyber protective barriers.

Additionally, it should be noted that these CDAs encompass those associated with physical security target sets.

- 6) A discussion of the licensee's cyber security program performance up to the date of the license amendment request.

The licensee stated there has been no identified compromise of SSEP functions by cyber means. It also noted a Quality Assurance (QA) audit was conducted in the last quarter of 2014, which included a review of the cyber security program implementation. There were no significant findings found related to cyber security program performance and effectiveness.

- 7) A discussion of cyber security issues pending in the licensee's corrective action program (CAP).

The licensee stated there are presently no significant (constituting a threat to a CDA via cyber means or calling into question program effectiveness) nuclear cyber security issues pending in the GGNS CAP. However, several non-significant issues identified during the QA audit, as described above and identified during NRC inspections have been entered into CAP.

- 8) A discussion of modifications completed to support the cyber security program and a discussion of pending cyber security modifications.

The licensee provided a brief discussion of a completed modification and pending modifications.

3.2 NRC Staff Evaluation

The NRC staff has evaluated the licensee's application using the regulatory requirements and guidance above. The NRC staff's evaluation is below. The NRC staff finds that the actions the licensee noted as being required to implement CSP, Section 3, "Analyzing Digital Computer Systems and Networks" and Section 4, "Establishing, Implementing and Maintaining the Cyber Security Program" are reasonable, as discussed below.

The licensee indicated that the activities described in Milestones 1 through 7 provide a high degree of protection of safety-related, important-to-safety, and security CDAs against common threat vectors. The NRC staff concludes that the licensee's site is more secure after the implementation of Milestones 1 through 7 because the activities the licensee has completed mitigate the most significant cyber attack vectors for the most significant CDAs. Therefore, the NRC has reasonable assurance that full implementation of the CSP by December 15, 2017, will provide adequate protection of the public health and safety and the common defense and security.

The licensee stated that the detail and depth of the technical analysis exceeds Entergy's prior understanding and necessitates a greater time and effort to achieve than Entergy anticipated when the current implementation schedule was developed. The NRC staff recognizes that CDA assessment work including application of controls is more complex and resource intensive than Entergy anticipated. As a result, the licensee has a large number of additional tasks not considered when developing its current CSP implementation schedule. The NRC staff

concludes that the licensee's request for additional time to implement Milestone 8 is reasonable given the complexity, volume, and scope of the remaining work required to fully implement its CSP.

The licensee proposed a Milestone 8 completion date of December 15, 2017. The licensee's prioritization of completion of work for CDAs follows the normal work management process that places the highest priority on apparent conditions adverse to quality in system, structure, and component design function and related to factors such as safety risk and nuclear defense-in-depth. High focus continues to be maintained on prompt attention to any emergent issue with safety-related, security and important-to-safety (including BOP) CDAs that would potentially challenge the established cyber protective barriers. The NRC staff concludes that the licensee's methodology for prioritizing work on CDAs is appropriate. The staff further concludes that the licensee's request to delay final implementation of the CSP until December 15, 2017, is reasonable given the complexity of the remaining work and the licensee's resource constraints.

3.3 Technical Evaluation Conclusion

Based on its review of the licensee's submittal, the NRC staff concludes that the licensee's request to delay full implementation of its CSP until December 15, 2017, is reasonable for the following reasons: (i) the licensee's implementation of Milestones 1 through 7 provides mitigation for significant cyber attack vectors for the most significant CDAs; (ii) the scope of the work required to come into full compliance with the CSP implementation schedule was much more complicated than the licensee anticipated when the current CSP implementation schedule was developed; and (iii) the licensee has reasonably prioritized and scheduled the work required to come into full compliance with its CSP implementation schedule. Therefore, the NRC staff finds the proposed change acceptable.

3.4 Revision to License Condition

By letter dated June 29, 2015, the licensee proposed to modify paragraph 2.E of FOL No. NPF-29, which provides a license condition requiring the licensee to fully implement and maintain in effect all provisions of the NRC-approved CSP.

The license condition in paragraph 2.E of FOL No. NPF-29 for GGNS is modified, in part, as follows:

The licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The licensee's CSP was approved by License Amendment No. 186 as supplemented by a change approved by License Amendment Nos. 192, 200, and 210.

4.0 REGULATORY COMMITMENTS

By letter dated June 29, 2015, the licensee made the following regulatory commitment:

Full implementation of the Grand Gulf Nuclear Station (GGNS) Cyber Security Plan for all safety, security, and emergency preparedness functions will be achieved.

Scheduled Completion Date: December 15, 2017

5.0 STATE CONSULTATION

In accordance with the Commission's regulations, the Mississippi State official was notified of the proposed issuance of the amendment. The State official had no comments.

6.0 ENVIRONMENTAL CONSIDERATION

This is an amendment to a 10 CFR Part 50 license that relates solely to safeguards matters and does not involve any significant construction impacts. This amendment is an administrative change to extend the date by which the licensee must have its CSP fully implemented. Accordingly, the amendment meets the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(12). Pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with the issuance of the amendment.

7.0 CONCLUSION

The Commission has concluded, based on the considerations discussed above, that: (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner, (2) there is reasonable assurance that 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.

Principal Contributor: J. Rycyna

Date: May 25, 2016

May 25, 2016

Vice President, Operations
Entergy Operations, Inc.
Grand Gulf Nuclear Station
P.O. Box 756
Port Gibson, MS 39150

SUBJECT: GRAND GULF NUCLEAR STATION, UNIT 1 - ISSUANCE OF AMENDMENT
RE: CYBER SECURITY PLAN MILESTONE 8 FULL IMPLEMENTATION
SCHEDULE (CAC NO. MF6566)

Dear Sir or Madam:

The U.S. Nuclear Regulatory Commission has issued the enclosed Amendment No. 210 to Facility Operating License No. NPF-29 for the Grand Gulf Nuclear Station, Unit 1 (GGNS). This amendment consists of changes to the facility operating license in response to your application dated June 29, 2015.

The amendment approves a change to the GGNS facility operating license to revise the Cyber Security Plan (CSP) Milestone 8 full implementation date from June 30, 2016 to December 15, 2017, as set forth in the CSP Implementation Schedule.

A copy of the related Safety Evaluation is enclosed. The Notice of Issuance will be included in the Commission's next biweekly *Federal Register* notice.

Sincerely,

/RA/

James Kim, Project Manager
Plant Licensing IV-2 and Decommissioning
Transition Branch
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-416

Enclosures:

1. Amendment No. 210 to NPF-29
2. Safety Evaluation

cc w/encls: Distribution via Listserv

DISTRIBUTION:

PUBLIC	RidsNrrPMGrandGulf Resource	RidsNsirOd Resource
LPL4-2 rff	RidsNrrLAPBlechman Resource	JBeardsley, NSIR
RidsNrrDorlDpr Resource	RidsRgn4MailCenter Resource	JRycyna, NSIR
RidsNrrDorlLpl4-2 Resource	RidsACRS_MailCTR Resource	

ADAMS Accession No. ML16119A148

*concurrence via email

OFFICE	NRR/DORL/LPL4-2/PM	NRR/DORL/LPL4-2/LA	NSIR/CSD/DD*
NAME	JKim	PBlechman	JBeardsley
DATE	5/3/16	5/2/16	4/15/16
OFFICE	OGC - NLO w/revision	NRR/DORL/LPL4-2/BC	NRR/DORL/LPL4-2/PM
NAME	JBielecki	MKhanna	JKim
DATE	5/16/16	5/19/16	5/25/16

OFFICIAL RECORD COPY