



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

December 12, 2014

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: MILESTONE 8 OF THE CYBER SECURITY PLAN (TAC NO. MF3325)

Dear Sir or Madam:

The Nuclear Regulatory Commission has issued the enclosed Amendment No. 200 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 December 19, 2013, as supplemented by letter dated June 11, 2014.

The amendment approves a change to the GGNS facility operating license to revise the date for implementation of Milestone 8 of the Cyber Security Plan (CSP) Implementation Schedule and the existing license conditions in the facility operating license. Milestone 8 of the CSP implementation schedule concerns the full implementation of the CSP.

A copy of our 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 "Alan Wang".

Alan B. Wang, 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. 200 to NPF-29
2. Safety Evaluation

cc w/encls: Distribution via Listserv



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

ENTERGY OPERATIONS, INC.

SYSTEM ENERGY RESOURCES, INC.

SOUTH MISSISSIPPI ELECTRIC POWER ASSOCIATION

ENTERGY MISSISSIPPI, INC.

DOCKET NO. 50-416

GRAND GULF NUCLEAR STATION, UNIT 1

AMENDMENT TO FACILITY OPERATING LICENSE

Amendment No. 200
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 December 19, 2013, as supplemented by letter dated June 11, 2014, 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 by changes to the facility operating license 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 No. 192 and 200.

3. This license amendment is effective as of its date of issuance and shall be implemented within 30 days from the date of issuance.

FOR THE NUCLEAR REGULATORY COMMISSION



Douglas A. Broaddus, 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: December 12, 2014

ATTACHMENT TO LICENSE AMENDMENT NO. 200

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

Insert

-16f-

-16f-

- (h) This license condition shall expire upon satisfaction of the requirements in paragraph (f) provided that a visual inspection of the steam dryer does not reveal any new unacceptable flaw or unacceptable flaw growth that is caused by fatigue.

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 No. 192 and 200.



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

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 200

TO FACILITY OPERATING LICENSE NO. NPF-29

ENTERGY OPERATIONS, INC., ET AL.

GRAND GULF NUCLEAR STATION, UNIT 1

DOCKET NO. 50-416

1.0 INTRODUCTION

By application dated December 19, 2013 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML14008A081), as supplemented by letter dated June 11, 2014 (ADAMS Accession No. ML14162A101), Entergy Operations Inc. (Entergy, the licensee), requested a change to the facility operating license (FOL) for the 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 supplemental letter dated June 11, 2011, provided additional information that clarified the application, did not expand the scope of the application as originally noticed, and did not change the U.S. Nuclear Regulatory Commission (NRC) staff's original proposed no significant hazards consideration determination as published in the *Federal Register* on July 8, 2014 (79 FR 38576).

Portions of the letter dated December 19, 2013, contain sensitive unclassified non-safeguards information and, accordingly, those portions are withheld from public disclosure in accordance with the provisions of paragraph 2.390(d)(1) of Title 10 of the *Code of Federal Regulations* (CFR).

2.0 REGULATORY EVALUATION

The NRC staff reviewed and approved the licensee's existing CSP implementation schedule in GGNS License Amendment No. 186 dated July 27, 2011 (ADAMS Accession No. ML111940165), concurrent with the incorporation of the CSP into the facility's current licensing bases. The NRC staff considered the following regulatory requirements and guidance in its review of the December 19, 2013, license amendment request (LAR) to modify the existing CSP implementation schedule:

- The regulations in 10 CFR 73.54, "Protection of digital computer and communication systems and networks," of 10 CFR state, in part, that: "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.
- In a publically available NRC memorandum dated October 24, 2013 (ADAMS Accession No. ML13295A467), the NRC staff listed criteria that it would consider during its evaluations of licensees' requests to postpone their cyber security programs 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 "[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 as required by 10 CFR 50.90.

3.0 TECHNICAL EVALUATION

3.1 Licensee's Requested Change

License Amendment No. 186 to FOL No. NPF-29 for GGNS was issued by the NRC staff on July 27, 2011. The NRC staff also approved the licensee's CSP implementation schedule, as discussed in the safety evaluation issued with the amendment. The implementation schedule had been submitted by the licensee based on a template prepared by the Nuclear Energy Institute (ADAMS Accession No. ML110600218), which the NRC staff found acceptable for licensees to use to develop their CSP implementation schedules. 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) Implement Installation of a deterministic one-way device 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) Commence ongoing monitoring and assessment activities for those target set CDAs whose security controls have been implemented; and
- 8) Full implementation of the CSP for all safety, security and emergency preparedness functions.

Currently, Milestone 8 of the GGNS CSP requires the licensee to fully implement the CSP by December 15, 2014. In its December 19, 2013, application, Entergy proposed to change the Milestone 8 completion date to June 30, 2016. The licensee's application addressed the eight criteria in the NRC's October 24, 2013, guidance memorandum.

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

- 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 specific requirements of the CSP that needs additional time to implement are Section 3, "Analyzing Digital Computer Systems and Networks," and Section 4, "Establishing, Implementing and Maintaining the Cyber Security Program." The licensee further stated that these sections describe requirements for application and maintenance of cyber security controls and describes the process of addressing security controls. The licensee described specific requirements needing additional time including determining the need for a specific security feature to provide for audit and accountability; monitoring tools and techniques; analyzing security alerts and advisories; and to assist personnel performing maintenance and testing activities. The licensee also described a need for additional physical controls for CDAs outside the security protected area and significant programmatic change management associated with approximately 40 procedure changes related to operational and management cyber security controls.

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

The licensee stated that it had a project team of approximately 20 personnel to perform and document the cyber security assessment process. However, even with that level of resource commitment, the analysis, which began in 2011, was not projected to be completed until the second quarter of 2014. Since the number of CDAs and existing procedures is in the hundreds and the number of individual cyber security control attributes is also in the hundreds, the total of physical, logical, and programmatic changes required, constitutes a significant project involving plant components and systems and substantial planning. Additionally, changes to CDAs and procedures must be integrated into the plant operational schedule including on-line operations, maintenance and testing, as well as planning and execution of refueling outages. With this analysis concluding in the second quarter of 2014, it is expected that insufficient time will remain in 2014 to conduct modification and change management planning activities and execution.

Further, the licensee intends to complete planning for the specific security feature, mentioned in Criterion (1) above, in 2014, and implement it in the following 18 months.

- 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 June 30, 2016, and stated that the revised Milestone 8 date will provide a 6-month contingency for the security feature mentioned in Criterion (1), above.

- 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 that the impact of the requested additional implementation time on the effectiveness of the overall cyber security program is considered to be very low, because milestones 1 through 7 have already been completed and have resulted in a high degree of protection of safety-related, important-to-safety, and security CDAs against common threat vectors. Additionally, 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 provided details about the implementation of the various milestones.

The NRC staff was concerned the LAR did not address all seven milestones and provided a request for additional information to the licensee on May 19, 2014 (ADAMS Accession No. ML14140A297). The licensee's response by letter dated June 11, 2014, indicated that all seven milestones had been implemented and the extension request had no effect on the milestones mentioned in the response.

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

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 Balance-of-Plant. Further, in regard to deterministic isolation and control of portable media devices (PMDs) for safety-related, important-to-safety (including Balance-of-Plant) and security CDAs, maintenance of one-way or air gapped configurations and implementation of control of PMDs remains high priority. This prioritization enabled completion of cyber security Interim Milestones 3 and 4 in 2012. 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 that there has been no identified compromise of safety, security, and emergency preparedness function by cyber means at GGNS. The licensee noted its experience with the scanning of portable devices. A formal Quality Assurance (QA) audit was conducted in the last quarter of 2013 that included review of the cyber security program implementation. There were no significant findings related to overall cyber security program performance and effectiveness.

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

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 corrective action program (CAP). Several non-significant issues identified during the QA audit described above, have been entered in the CAP. Additionally, when the internal NRC memorandum entitled, "Enhanced Guidance for Licensee Near-Term Corrective Actions to Address Cyber Security Inspection Findings and Licensee Eligibility for 'Good-Faith' Attempt Discretion" (not publicly available; security related), dated July 1, 2013, was shared with Entergy, the actions described regarding cyber security Interim Milestone 4 were entered in the CAP for evaluation by the CSAT. Final actions regarding some program activities are pending.

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

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

3.2 NRC Staff Evaluation

The NRC staff has evaluated the licensee's application using the regulatory requirements and the guidance above in Section 2.0 of this safety evaluation. The NRC staff's evaluation is below.

The licensee indicated that the milestones already completed have resulted in a high degree of protection of safety-related, important-to-safety, and security CDAs against threat vectors. The licensee detailed activities completed for each milestone. The NRC staff finds that the licensee's site is much more secure after implementation of Milestones 1 through 7 because the activities the licensee 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 June 30, 2016 will provide adequate protection of the public health and safety and the common defense and security.

The licensee stated that there is insufficient time remaining in 2014 to complete the scope of actions required to fully implement its CSP (the cyber security assessment process). The NRC staff recognizes that cyber security assessment work is much more complex and resource intensive than originally anticipated, in part due to the NRC expanding the scope of the cyber security requirements to include balance of plant. As a result, the licensee has a large number of additional tasks not originally considered when developing its CSP implementation schedule.

The licensee proposed a Milestone 8 completion date of June 30, 2016. The licensee stated that changing the completion date of Milestone 8 allows for designing and planning for security features to fully implement the security controls required by the CSP. It also allows for activities that require a refueling outage for implementation. The licensee stated its methodology for prioritization 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 factors such as safety risk and nuclear defense-in-depth, as well as threats to continuity of electric power generation in the Balance-of-Plant. The NRC staff concludes that based on the large number of digital assets described above and the limited resources with the appropriate expertise to perform these activities, the licensee's methodology for prioritizing work on CDAs is appropriate. The NRC staff further concludes that the licensee's request to delay final implementation of the CSP until June 30, 2016, is reasonable given the complexity of the remaining unanticipated work and the need to perform certain work during the scheduled refueling outage.

3.3 Technical Evaluation Conclusion

The NRC staff concludes that the licensee's request to delay full implementation of its CSP until June 30, 2016, 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 as discussed in the staff evaluation above; (ii) the scope of the work required to come into full compliance with the CSP implementation schedule was much more complicated than anticipated and not reasonably foreseeable when the CSP implementation scheduled was originally developed; and (iii) the licensee has reasonably prioritized and scheduled the work required to come into full compliance with its CSP implementation schedule.

3.4 Revision to License Condition

By letter dated December 19, 2013, the licensee proposed to modify Paragraph 2.E of FOL No. NPF-29 for GGNS, which provides a license condition to require 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 No. 192 and 200.

3.5 Regulatory Commitment

By letter dated December 19, 2013, Entergy made the following regulatory commitment, with a scheduled completion date of June 30, 2016:

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

4.0 STATE CONSULTATION

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

5.0 ENVIRONMENTAL CONSIDERATION

This amendment to a Part 50 license 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 cyber security plan fully implemented. The Commission has previously issued a proposed finding that the amendments involve no significant hazards consideration, and there has been no public comment on such finding published in the *Federal Register* on July 8, 2014 (79 FR 38576). 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.

6.0 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: December 12, 2014

December 12, 2014

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: MILESTONE 8 OF THE CYBER SECURITY PLAN (TAC NO. MF3325)

Dear Sir or Madam:

The Nuclear Regulatory Commission has issued the enclosed Amendment No. 200 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 December 19, 2013, as supplemented by letter dated June 11, 2014.

The amendment approves a change to the GGNS facility operating license to revise the date for implementation of Milestone 8 of the Cyber Security Plan (CSP) Implementation Schedule and the existing license conditions in the facility operating license. Milestone 8 of the CSP implementation schedule concerns the full implementation of the CSP.

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

Sincerely,
/RA/

Alan B. Wang, 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. 200 to NPF-29
- 2. Safety Evaluation

cc w/encls: Distribution via Listserv

DISTRIBUTION:

PUBLIC RidsNrrLAJBurkhardt Resource RidsAcrsAcnw_MailCTR Resource
LPL4-2 r/f RidsNrrPMGrandGulf Resource RidsNsrOd Resource
RidsNrrDorlDpr Resource RidsNrrLAPBlechman Resource JRycyna, NSIR
RidsNrrDorlLp4-2 Resource RidsRgn4MailCenter Resource

ADAMS Accession No. ML14311A479

*concurrence via email

OFFICE	NRR/DORL/LPL4-2/PM	NRR/DORL/LPL4-2/LA	NRR/DORL/LPL4-2/LA	NSIR/CSD/DD*
NAME	AWang	PBlechman	JBurkhardt	RFelts
DATE	12/11/2014	11/12/14	11/25/14	11/5/14
OFFICE	OGC	NRR/DORL/LPL4-2/BC	NRR/DORL/LPL4-2/PM	
NAME	LSClark	DBroaddus	AWang	
DATE	12/10/14	12/11/2/14	12/12/14	

OFFICIAL RECORD COPY