



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

December 12, 2014

Vice President, Operations  
Entergy Operations, Inc.  
River Bend Station  
5485 US Highway 61N  
St. Francisville, LA 70775

SUBJECT: RIVER BEND STATION, UNIT 1 - ISSUANCE OF AMENDMENT RE:  
MILESTONE 8 OF THE CYBER SECURITY PLAN (TAC NO. MF3492)

Dear Sir or Madam:

The U.S. Nuclear Regulatory Commission (the Commission) has issued the enclosed Amendment No. 184 to Facility Operating License No. NPF-47 for the River Bend Station, Unit 1 (RBS). The amendment consists of changes to the facility operating license in response to your application dated February 25, 2014.

The amendment approves a change to the RBS 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. 50-458

Enclosures:

1. Amendment No. 184 to NPF-47
2. Safety Evaluation

cc w/encls: Distribution via Listserv



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

ENTERGY GULF STATES LOUISIANA, LLC

AND

ENTERGY OPERATIONS, INC.

DOCKET NO. 50-458

RIVER BEND STATION, UNIT 1

AMENDMENT TO FACILITY OPERATING LICENSE

Amendment No. 184  
License No. NPF-47

1. The Nuclear Regulatory Commission (the Commission) has found that:
  - A. The application for amendment by Entergy Operations, Inc. (the licensee), dated February 25, 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, as amended, 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 license 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 as indicated in the attachment to this license amendment, and Paragraph 2.E of Facility Operating License No. NPF-47 is hereby amended to read as follows:
  - E. 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. 171 as supplemented by a change approved by License Amendment No. 184.
3. The license amendment is effective as of its date of issuance and shall be implemented within 60 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-47

Date of Issuance: December 12, 2014

ATTACHMENT TO LICENSE AMENDMENT NO. 184

FACILITY OPERATING LICENSE NO. NPF-47

DOCKET NO. 50-458

Replace the following page of the Facility Operating License No. NPF-47 with the attached revised page. The revised page is identified by Amendment number and contains marginal lines indicating the areas of change.

Facility Operating License

Remove

Insert

-7-

-7-

- D. 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 the 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 combined set of plans, which contain Safeguards Information protected under 10 CFR 73.21, is entitled: "Physical Security, Safeguards Contingency and Training & Qualification Plan," submitted by letter dated May 16, 2006.
- E. 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. 171 as supplemented by a change approved by License Amendment No. 184.
- F. Except as otherwise provided in the Technical Specifications or Environmental Protection Plan, EOI shall report any violations of the requirements contained in Section 2, Items C.(1) C.(3) through (9) and C.(11) through (16) of this license in the following manner: initial notification shall be made within 24 hours to the NRC Operations Center via the Emergency Notification System with written followup within 60 days in accordance with the procedures described in 10 CFR 50.73(b), (c) and (e).
- G. The licensee 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.
- H. This license is effective as of the date of issuance and shall expire at midnight on August 29, 2025.

FOR THE NUCLEAR REGULATORY COMMISSION

Harold R. Denton, Director  
Office of Nuclear Reactor Regulation

Enclosures:

- 1. Attachments 1-5
- 2. Appendix A - Technical Specifications (NUREG-1172)
- 3. Appendix B - Environmental Protection Plan
- 4. Appendix C - Antitrust Conditions

Date of Issuance: November 20, 1985

Revised: December 16, 1993

Amendment No. ~~70-79-85-119-135-171-177~~, 184  
Revised by letter dated October 28, 2004  
Revised by letter dated November 19, 2004  
Revised by letter dated January 24, 2007



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

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 184 TO

FACILITY OPERATING LICENSE NO. NPF-47

ENTERGY OPERATIONS, INC.

RIVER BEND STATION, UNIT 1

DOCKET NO. 50-458

1.0 INTRODUCTION

By application dated February 25, 2014 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML14064A349), Entergy Operations, Inc. (Entergy, the licensee), requested a change to the facility operating license (FOL) for the River Bend Station, Unit 1 (RBS). 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.

Portions of the letter dated February 25, 2014, 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* (10 CFR).

2.0 REGULATORY EVALUATION

The U.S. Nuclear Regulatory Commission (NRC, the Commission) staff reviewed and approved the licensee's existing CSP implementation schedule in RBS License Amendment No. 171 dated July 29, 2011 (ADAMS Accession No. ML111940200), 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 current license amendment request to modify the existing CSP implementation schedule:

- The regulations in 10 CFR 73.54, "Protection of digital computer and communication systems and networks," of 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 dates (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

Amendment No. 171 to FOL NPF-47 for RBS was issued by the NRC staff on July 29, 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 (NEI) (ADAMS Accession No. ML110600218), which the NRC staff found acceptable for licensees to use to develop their CSP implementation schedules (ADAMS Accession No. ML110070348). 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 data diode 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;
- 6) Identify, document, and implement 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;
- 8) Fully implement the CSP.

Currently, Milestone 8 of the RBS CSP requires the licensee to fully implement the CSP by December 15, 2014. In its February 25, 2014, application, the licensee proposed to change the Milestone 8 completion date to June 30, 2016.

The licensee provided the following information pertinent to each of the eight evaluation criteria identified in the NRC guidance memorandum.

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 CSP Sections 3 and 4 describe requirements for application and maintenance of security controls listed in NEI 08-09, Revision 6, "Cyber Security Plans for Nuclear Power Reactors," Appendices D and E. The licensee provided a list of specific requirements needing additional time.

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

The licensee stated it had a robust full-time team of approximately 20 personnel to perform and document the detailed analysis (cyber security assessment process). The licensee explained that even with that level of resource commitment, the analysis, which began in 2011, was projected to be completed by the second quarter of 2014. This analysis compares CDAs to the Technical Cyber Security controls described in NEI 08-09, Revision 6, Appendix D, and compares existing practices, programs, and procedures to the Operational and Management Cyber Security Controls described in NEI 08-09, Revision 6, Appendix E. The output of this process includes identification of specific remediation actions required to close gaps and satisfy each control. 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 the analysis not anticipated to conclude until 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. The licensee's revised CSP implementation schedule notes the proposed date provides for activities that require a refueling outage.

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 said this is based on designing and planning modifications in 2014 and installing them in 2015, with an additional contingency of 6 months.



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 considered to be very low, because the milestones already completed have resulted in a high degree of protection of safety-related, important-to-safety, and security CDAs against 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.

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

The licensee stated 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. This prioritization enabled completion of cyber security Milestones 3 and 4 in 2012. Heightened attention is being maintained for any emergent issues with these CDAs that would potentially challenge the established cyber protective barriers. Additionally, in regard to deterministic isolation and control of portable media devices for safety-related, important-to-safety and security CDAs, maintenance of one-way or air gapped configurations and implementation of control of portable media devices is a high priority.

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 (SSEP) function by cyber means at any Entergy plant. A formal Quality Assurance (QA) audit was conducted in the fourth quarter of 2013 pursuant to the 24-month physical security program review required by 10 CFR 73.55(m). The QA audit included review of 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 into CAP for evaluation by the CSAT. The licensee also provided an example of cyber security issues in the 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 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. The NRC staff has concluded that the additional time the licensee noted as being required to implement security controls is reasonable as discussed 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 NRC staff finds these actions provide a high degree of protection to ensure that the most significant digital computer and communication systems and networks associated with SSEP systems are already protected against cyber attacks. 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.

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

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 as well as the number of individual cyber security control attributes that need to be considered, and the fact that changes to CDAs and procedures must be integrated into the plant operational schedule including on-line operations, maintenance, and testing, 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 schedule 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. 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.

### 3.4 Revision to License Condition 2.E

By letter dated February 25, 2014, the licensee proposed to modify Paragraph 2.E of FOL No. NFP-47 for RBS, 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. NFP-47 for RBS is modified to read as follows:

- E. 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. 171 as supplemented by a change approved by License Amendment No. 184.

### 3.5 Regulatory Commitment

In letter dated February 25, 2014, Entergy made the following regulatory commitment, with a completion date of June 30, 2016:

Full implementation of *River Bend Station (RBS) 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 is an amendment of 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. The

Commission has previously issued a proposed finding that the amendment involves no significant hazards consideration, and there has been no public comment on such finding published in the *Federal Register* on July 8, 2014 (79FR 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.  
River Bend Station  
5485 US Highway 61N  
St. Francisville, LA 70775

SUBJECT: RIVER BEND STATION, UNIT 1 - ISSUANCE OF AMENDMENT RE:  
MILESTONE 8 OF THE CYBER SECURITY PLAN (TAC NO. MF3492)

Dear Sir or Madam:

The U.S. Nuclear Regulatory Commission (the Commission) has issued the enclosed Amendment No. 184 to Facility Operating License No. NPF-47 for the River Bend Station, Unit 1 (RBS). The amendment consists of changes to the facility operating license in response to your application dated February 25, 2014.

The amendment approves a change to the RBS 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. 50-458

Enclosures:

1. Amendment No. 184 to NPF-47
2. Safety Evaluation

cc w/encls: Distribution via Listserv

DISTRIBUTION:

PUBLIC  
LPL4-2 r/f  
RidsAcrsAcnw\_MailCTR Resource  
RidsNrrDssStsb Resource

RidsNrrDorlDpr Resource  
RidsNrrDorlLpl4-2 Resource  
RidsNrrLAJBurkhardt Resource  
RidsNrrPMRiverBend Resource

RidsRgn4MailCenter Resource  
JRycyna, NSIR/CSD

ADAMS Accession No. ML14304A181

\*concurrence via email \*\*NLO via email

OFFICE	NRR/DORL/LPL4-2/PM	NRR/DORL/LPL4-2/LA	NSIR/CSD/DD*
NAME	ABWang	JBurkhardt	BWestreich
DATE	11/4/14	10/31/14	10/24/14
OFFICE	OGC**	NRR/DORL/LPL4-2/BC	NRR/DORL/LPL4-2/PM
NAME	NStAmour	DBroaddus (MOrenak for)	ABWang
DATE	12/5/2104	12/12/14	12/12/14

OFFICIAL AGENCY RECORD