Entergy

Entergy Operations, Inc.
River Bend Station
5485 U.S. Highway 61N
St. Francisville, LA 70775
Tel: 225-381-4374

Eric W. Olson
Site Vice President

RBG-47630
RBF1-15-0181

December 3, 2015

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

SUBJECT: Resubmittal of License Amendment Request – Cyber Security Plan Implementation Schedule
River Bend Station - Unit 1
License No. NPF-47
Docket No. 50-458

REFERENCES:

1. NRC Internal Memorandum to Barry Westreich from Russell Felts, *Review Criteria for 10 CFR 73.54, Cyber Security Implementation Schedule Milestone 8 License Amendment Requests*, dated October 24, 2013 (ADAMS Accession No. ML13295A467)

2. NRC letter to Entergy, *Issuance of Amendment Re: Approval of Cyber Security Plan*, dated July 29, 2011 (RBC-50945)

3. NRC letter to Entergy, *Issuance of Amendment Re: Approval of Cyber Security Plan*, dated December 12, 2014 (RBC-51271) (ADAMS Accession No. ML14304A181)

4. NRC internal memorandum from the Director Cyber Security Directorate, Office of Nuclear Security and Incident Response, to the Region I through IV Directors of Reactor Safety, Enhanced Guidance for Licensee Near-Term Corrective Actions to Address Cyber Security Inspection Findings and Licensee Eligibility for "Good-Faith" Attempt Discretion, Enclosure 2, Milestone 4 Resolution Actions, dated July 1, 2013

S001A
NRR

Dear Sir or Madam:

This letter is provided to replace prior submittal, "License Amendment Request Cyber Security Plan Implementation Schedule," dated June 29, 2015 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML15188A369). This submittal contains administrative changes by removing Safeguards level of information only and does not change the technical content of the original.

Pursuant to 10 CFR 50.4 and 10 CFR 50.90, Entergy Operations, Inc. (Entergy) hereby requests an amendment to the Renewed Facility Operating License for River Bend Station (RBS). In accordance with the guidelines provided by Reference 1, this request proposes a change to the RBS Cyber Security Plan Milestone 8 full implementation date as set forth in the Cyber Security Plan Implementation Schedule approved by References 2 and 3.

Attachment 1 provides an evaluation of the proposed change. Attachment 2 contains proposed marked-up operating license pages for the Physical Protection license condition for River Bend Station to reference the commitment change provided in this submittal.

Attachment 3 contains the proposed revised operating license pages. Attachment 4 contains a change to the date of Implementation Milestone 8.

The proposed changes have 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 the changes involve no significant hazards consideration. The bases for these determinations are included in Attachment 1.

Entergy requests this license amendment be effective as of its date of issuance. Although this request is neither exigent nor emergency, your review and approval is requested prior to June 30, 2016.

The revised commitment contained in this submittal is summarized in Attachment 5. Should you have any questions concerning this letter, or require additional information, please contact Mr. Joseph Clark at (225)381-4177.

I declare under penalty of perjury that the foregoing is true and correct. Executed on November 16, 2015.

Sincerely,

Eric W. Olson

TSH

EWO/JAC/tjb

Attachments:
1. Analysis of Proposed Operating License Change
2. Proposed RBS Operating License Change (mark-up)
3. Revised RBS Operating License Page
4. Revised Cyber Security Plan Implementation Schedule
5. List of Regulatory Commitments

cc: Regional Administrator
U. S. Nuclear Regulatory Commission
Region IV
1600 East Lamar Boulevard
Arlington, TX 76011-4511

NRC Senior Resident Inspector
PO Box 1050
St. Francisville, LA 70775

U. S. Nuclear Regulatory Commission
Attn: Mr. Stephen Koenick, Project Manager
MS 8 B1A
One White Flint North
11555 Rockville Pike
Rockville, MD 20852

U. S. Nuclear Regulatory Commission
Attn: Mr. Alan B. Wang, Project Manager
MS O-8 B1
One White Flint North
11555 Rockville Pike
Rockville, MD 20852

Ji Young Wiley (w/o Attachments 1 and 4)
Louisiana Department of Environmental Quality
Office of Environmental Quality
P. O. Box 4312
Baton Rouge, LA 70821-4312

Central Records Clerk (w/o Attachments 1 and 4)
Public Utility Commission of Texas
1701 N. Congress Ave.
Austin, TX 78711-3326

Attachment 1

RBG-47630

Analysis of Proposed Operating License Change

1.0 SUMMARY DESCRIPTION

This license amendment request (LAR) includes a proposed change to the RBS Cyber Security Plan (CSP) Implementation Schedule Milestone 8 full implementation date and a proposed revision to the existing operating license Physical Protection license condition.

2.0 DETAILED DESCRIPTION

In Reference 1, the NRC provided criteria to be used for evaluation of a license amendment request to revise the Cyber Security Implementation Schedule Milestone 8 date. In Reference 3, the NRC issued a license amendment to the Facility Operating License for RBS that approved the RBS CSP and associated implementation milestone schedule. The CSP Implementation Schedule approved by Reference 3 was utilized as a portion of the basis for the NRC's safety evaluation report provided by Reference 3. Entergy Operations, Inc. (Entergy) is proposing a change to the Milestone 8 date from June 30, 2016, to December 15, 2017, for full implementation of the CSP for all applicable safety, security, and emergency preparedness (SSEP) functions.

3.0 TECHNICAL EVALUATION

Below is Entergy's discussion of the eight evaluation criteria provided by Reference 1:

1. **Identification of the specific requirement or requirements of the CSP that the licensee needs additional time to implement.**

   The CSP Sections 3 and 4 describe requirements for application and maintenance of cyber security controls listed in Nuclear Energy Institute (NEI) 08-09, Revision 6, *Cyber Security Plan for Nuclear Power Reactors*, Appendices D and E. Application of the controls is accomplished after completion of detailed analyses (the cyber security assessment process) that identify "gaps," or the difference between current configuration and a configuration that satisfies each cyber security control. Gap closure can require any combination of physical, logical (software-related), or programmatic/procedural changes.

   a. Entergy is in the process of determining the need for automated security information and event management (SIEM) systems, and designing/implementing these systems for monitoring activity on networks of critical digital assets (CDAs), pursuant to NEI 08-09, Revision 6, Appendix D-2 (Audit and Accountability), and Appendices E-3.4 (Monitoring Tools and Techniques), 3.5 (Security Alerts and Advisories), and 4.3 (Personnel Performing maintenance and Testing Activities)

   b. Additional physical controls for CDAs outside the security protected area pursuant to NEI 08-09, Revision 6, Appendix E-5.1 (Physical and Operational Environment Protection Policies and Procedures)

c. Significant programmatic change management associated with approximately 40 procedure changes pursuant to NEI 08-09, Revision 6, Appendix E (Operational and Management Cyber Security Controls).

2. Detailed justification that describes the reason additional time is required to implement the specific requirement or requirements identified.

a. Entergy hosted a "pilot" Milestone 8 inspection at the Indian Point site in March 2014. During the pilot, insight was gained into NRC interpretation on how to apply the cyber security controls listed in NEI 08-09, Revision 6. These interpretations were not previously available. During the pilot inspection, the NRC team reviewed several examples of critical digital assets (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, it is evident to Entergy that the detail and depth of the technical analysis exceeds Entergy's prior understanding and requires a considerably greater effort to achieve than initially anticipated.

b. During 2015, each operating Entergy licensee has an inspection of compliance with interim Milestones 1 through 7. The preparation for and support of these inspections has 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.

c. Development of an endorsed written standard for interpreting and applying the NEI 08-09 cyber security controls has continued to be a work-in-progress over the past five years. NEI 13-10, Revision 2, a guideline intended to provide some reduction of controls implementation based on equipment safety significance, has been endorsed. However, an initial screening of Entergy CDAs using this guideline indicates the reduction in both analytical work and actual application of controls would not be significant.

d. In June 2014, NEI submitted a petition for rulemaking to the Commission. The petition was subsequently found acceptable for review. The petition proposes a change to the rule to more precisely align the scope of the rule with the underlying objective of preventing radiological sabotage, which NEI estimates could potentially result in a reduction in the scope of cyber security implementation. While Entergy does not intend to suspend any implementation work in anticipation of the petition being approved, the petition being submitted is indicative that the final process for implementing the rule has not stabilized, and therefore, Entergy requires additional time to receive any implementation benefit from such rulemaking.

e. Benchmarking data gathered on Milestone 8 implementation schedules for non-Entergy licensees indicates that a significant number of licensees have either gained approval for a new Milestone 8 date or submitted an extension request significantly beyond Entergy's current due date; therefore, Entergy's request is consistent with the industry.

3. **Proposed completion date for Milestone 8 consistent with the remaining scope of work to be conducted and the resources available.**

   The proposed completion date for Milestone 8 is December 15, 2017.

4. **Evaluation of the impact that the additional time to implement the requirements will have on the effectiveness of the overall cyber security program in the context of milestones already completed.**

   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 Interim Milestones already completed have resulted in a high degree of protection of safety-related, important-to-safety, and security CDAs against threat vectors associated with external connectivity (both wired and wireless), and portable digital media and devices. Additionally, extensive physical and administrative measures are already in place for CDAs pursuant to the RBS Security Plan and Technical Specification requirements. In the context of cyber security milestones already completed, the following is noted:

   a. An Entergy Cyber Security Assessment Team (CSAT) has been implemented consisting of highly experienced personnel knowledgeable in reactor and balance-of-plant design, licensing, safety, security, emergency preparedness, information technology, and cyber security. The CSAT is provided with the authority, via written procedure, to perform the analyses and oversight activities described in the CSP. Entergy employs a single overall fleet-wide CSAT to ensure consistency of results among the fleet.

   b. Critical systems and CDAs have been identified, documented, and entered in a controlled database.

   c. The plant process computer network and the plant security computer network have been deterministically isolated per the requirements of cyber security Interim Milestone 3.

   d. Safety-related, important-to-safety, and security CDAs have been extensively reviewed and verified (or modified) to be deterministically isolated and not to employ wireless network technology.

   e. Procedures have been implemented for portable digital media and devices periodically connected to CDAs, per NEI 08-09, Revision 6, Appendix D, Section 1.19.

   f. CDAs associated with physical security target sets have been analyzed per the requirements of the CSP Section 3.1.6 and either (1) verified to satisfy the Technical Cyber Security Controls described in NEI 08-09, Revision 6, Appendix D or (2) actions required to satisfy the Technical Cyber Security

Controls described in NEI 08-09, Revision 6, Appendix D, are captured in the Corrective Action Program.

g. Employees have been provided with training on cyber security awareness, tampering, and control of portable digital media and devices periodically connected to CDAs.

h. Entergy has transitioned from the previous cyber security program described by NEI 04-04. Revisions have been made to procedures that control plant modifications, planning, and maintenance, establishing ties to cyber security procedures for CDA analysis and control of portable digital media and devices periodically connected to CDAs.

5. **Description of the methodology for prioritizing completion of work for CDAs associated with significant SSEP consequences and with reactivity effects in the balance of plant.**

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 (BOP). Further, in regard to deterministic isolation and control of portable media devices (PMD) for safety-related, important-to-safety (including BOP), and security CDAs, maintenance of one-way or air-gapped configurations and implementation of control of PMD remains a high priority. This prioritization enabled completion of cyber security Interim Milestones 3 and 4. 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. **Discussion of the cyber security program performance up to the date of the license amendment request.**

No compromise of SSEP function by cyber means has been identified. Additionally, a Quality Assurance (QA) audit was conducted in the fourth quarter of 2014 pursuant to the 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. **Discussion of cyber security issues pending in the corrective action program.**

No significant (with 'significant' meaning constituting a threat to a CDA via cyber means or calling into question program effectiveness) nuclear cyber security issues are currently pending in the CAP. Several non-significant issues identified during the QA audit described above and identified during NRC inspections of compliance with nuclear cyber security Interim Milestones 1 through 7 have been entered into CAP. However, when the Reference 4 internal NRC memorandum was shared with Entergy, the actions described regarding cyber security Interim Milestone 4 were entered into CAP for evaluation by the CSAT.

8. **Discussion of modifications completed to support the cyber security program and a discussion of pending cyber security modifications.**

   Modifications completed include those required to deterministically isolate the Level 3 and 4 CDAs, as required by Interim Milestone 3, by data diode or air gap. Potential modifications not yet implemented include automated security information event monitoring systems for monitoring activity on networks of CDAs, pursuant to NEI 08-09, Revision 6, Appendix D-2 (Audit and Accountability), and Appendices E-3.4 (Monitoring Tools and Techniques), 3.5 (Security Alerts and Advisories), and 4.3 (Personnel Performing Maintenance and Testing Activities), and additional physical controls for CDAs outside the Protected Area pursuant to NEI 08-09, Revision 6, Appendix E-5.1 (Physical and Operational Environment Protection Policies and Procedures).

This LAR includes the proposed change to the existing operating license condition for "Physical Protection" (Attachments 2 and 3) for RBS. This LAR also contains the proposed Revised CSP Implementation Schedule (Attachment 4), and this LAR also provides a revised list of regulatory commitments (Attachment 5).

4.0 REGULATORY EVALUATION

4.1 Applicable Regulatory Requirements/Criteria

10 CFR 73.54 requires licensees to maintain and implement a cyber security plan (CSP). RBS Facility Operating License No. NPF-47, includes a Physical Protection license condition that requires Entergy Operations, Inc. (Entergy) to fully implement and maintain in effect all provisions of the Commission-approved CSP, including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p).

4.2 Significant Safety Hazards Consideration

Entergy is requesting an amendment to the NPF-47 Facility Operating License to revise the Physical Protection license condition as it relates to the CSP. This change includes a proposed change to a CSP Implementation Schedule milestone date and a proposed revision to the NPF-47 Facility Operating License to include the proposed deviation. Specifically, Entergy is proposing a change to the Implementation Milestone 8 completion date.

Entergy has evaluated whether or not a significant hazards consideration is involved with the proposed amendment by focusing on the three standards set forth in 10 CFR 50.92, "Issuance of Amendment," as discussed below:

1. Does the proposed change involve a significant increase in the probability or consequences of an accident previously evaluated?

   Response: No.

   The proposed change to the CSP Implementation Schedule is administrative in nature. This change does not 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 proposed change does not require any plant modifications which affect the performance capability of the structures, systems, and components relied upon to mitigate the consequences of postulated accidents and has no impact on the probability or consequences of an accident previously evaluated.

Therefore, the proposed change does not involve a significant increase in the probability or consequences of an accident previously evaluated.

2. Does the proposed change create the possibility of a new or different kind of accident from any accident previously evaluated?

Response: No.

The proposed change to the CSP Implementation Schedule is administrative in nature. This proposed change does not 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 proposed change does not require any plant modifications which affect the performance capability of the structures, systems, and components relied upon to mitigate the consequences of postulated accidents and does not create the possibility of a new or different kind of accident from any accident previously evaluated.

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

3. Does the proposed change involve a significant reduction in a margin of safety?

Response: No.

Plant safety margins are established through limiting conditions for operation, limiting safety system settings, and safety limits specified in the technical specifications. The proposed change to the CSP Implementation Schedule is administrative in nature. In addition, the milestone date delay for full implementation of the CSP has no substantive impact because other measures have been taken which provide adequate protection during this period of time. Because there is no change to established safety margins as a result of this change, the proposed change does not involve a significant reduction in a margin of safety.

Therefore, 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 provides a change to the CSP Implementation Schedule. The proposed amendment meets the eligibility criterion for a categorical exclusion set forth in 10 CFR 51.22(c)(12). Therefore, 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 REFERENCES

1. NRC Internal Memorandum to Barry Westrich from Russell Felts, *Review Criteria for 10 CFR 73.54, Cyber Security Implementation Schedule Milestone 8 License Amendment Requests*, dated October 24, 2013

2. NRC letter to Entergy, *Issuance of Amendment Re: Approval of Cyber Security Plan*, dated July 29, 2011 (RBC-50945)

3. NRC letter to Entergy, *Issuance of Amendment Re: Approval of Cyber Security Plan*, dated December 12, 2014 (ADAMS Accession No. ML14304A181)

4. NRC internal memorandum from the Director Cyber Security Directorate, Office of Nuclear Security and Incident Response, to the Region I through IV Directors of Reactor Safety, *Enhanced Guidance for Licensee Near-Term Corrective Actions to Address Cyber Security Inspection Findings and Licensee Eligibility for "Good-Faith" Attempt Discretion, Enclosure 2, Milestone 4 Resolution Actions*, dated July 1, 2013

Attachment 2

RBG-47630

Proposed River Bend Station Operating License Change (mark-up)

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 changes approved by License Amendment Nos. 184, and xxx.

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

Attachment 3

RBG-47630

Revised River Bend Station Operating License Page

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 changes approved by License Amendment Nos. 184, and XXX.

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:
5. Attachments 1-5
6. Appendix A - Technical Specifications (NUREG-1172)
7. Appendix B - Environmental Protection Plan
8. Appendix C - Antitrust Conditions

Date of Issuance: November 20, 1985

Revised: December 16, 1993

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

Attachment 5

RBG-47630

List of Regulatory Commitments

List of Regulatory Commitments

The following table identifies those actions committed to by Entergy in this document. Any other statements in this submittal are provided for information purposes and are not considered to be regulatory commitments.

COMMITMENT	TYPE (Check One)		SCHEDULED COMPLETION DATE (If Required)
	ONE-TIME ACTION	CONTINUING COMPLIANCE	
Full implementation of *RBS Cyber Security Plan* for all safety, security, and emergency preparedness functions will be achieved.	X		December 15, 2017

Attachment 4

RBG-47630

Revised Cyber Security Plan Implementation Schedule

Revised Cyber Security Plan Implementation Schedule

#	Implementation Milestone	Completion Date	Basis
8	Full implementation of *River Bend Station (RBS) Cyber Security Plan* for all safety, security, and emergency preparedness (SSEP) functions will be achieved.	December 15, 2017	By the completion date, the RBS Cyber Security Plan will be fully implemented for all SSEP functions in accordance with 10 CFR 73.54. This date also bounds the completion of all individual asset security control design remediation actions including those that require a refueling outage for implementation.