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

September 16, 2026

EAF-RIV-2026-0049

Phil Hansett, Site Vice President
Entergy Operations, Inc.
5485 U.S. Highway 61N
St. Francisville, LA 70775

SUBJECT: RIVER BEND STATION – NRC INSPECTION REPORT 05000458/2026092 AND INVESTIGATION REPORT OI-RIV-2025-0094

Dear Phil Hansett:

This letter refers to an investigation completed on May 11, 2026, by the U.S. Nuclear Regulatory Commission's (NRC's) Office of Investigations at River Bend Station (RBS). The investigation was conducted to determine whether a maintenance supervisor (a member of the critical group) and a contractor (a non-critical group member) engaged in deliberate misconduct when the critical group member transferred a critical digital asset (CDA) cybersecurity key, along with his site access badge, to the non-critical group member. The issue was discussed with Rob Melton, General Manager Plant Operations (GMPO) and other members of your staff during a technical debrief on August 26, 2026. A factual summary of the investigation is provided as Enclosure 1.

Based on the results of this investigation, one apparent violation was identified and is being considered for escalated enforcement action in accordance with the NRC Enforcement Policy. The current Enforcement Policy is included on the NRC's website at http://www.nrc.gov/about-nrc/regulatory/enforcement/enforce-pol.html. The apparent violation involves the failure to implement a cyber security plan as required by 10 CFR 73.54(b)(2). The circumstances surrounding the apparent violation, the significance of the issues, and the need for lasting and effective corrective action were discussed with members of your staff at the inspection exit meeting on August 31, 2026. Further details regarding the apparent violation are documented in Enclosure 2 of this letter.

Before the NRC makes its enforcement decision, we are providing you an opportunity to (1) respond in writing to the apparent violation in Enclosure 2 of this letter within 30 days of the date of this letter, (2) request a predecisional enforcement conference (PEC), or (3) request alternative dispute resolution (ADR). If a PEC is held, the NRC will issue a press release to announce the time and date of the conference; however, the PEC will be closed to public observation since information related to an Office of Investigations report will be discussed and the report has not been made public. Please contact Shiattin Makor, Chief, Engineering Branch, at 817-200-1507 or at Shiattin.Makor@nrc.gov within 10 days of the date of this letter to notify the NRC of your intent to either provide a written response, participate in a PEC, or request ADR. A PEC should be held within 30 days and an ADR session within 45 days of the date of this letter.

If you choose to send a written response, it should be clearly marked as a “Response to Apparent Violation in NRC Inspection Report 05000458/2026092 and Investigation Report OI-RIV-2025-0094; EAF-RIV-2026-0049” and should include: (1) the reason for the apparent violation or, if contested, the basis for disputing the apparent violation; (2) the corrective steps that have been taken and the results achieved; (3) the corrective steps that will be taken; and (4) the date when full compliance will be achieved. Your response may reference or include previously docketed correspondence if the correspondence adequately addresses the required response. Your response should be sent to the Director, Division of Reactor Safety, U.S. Nuclear Regulatory Commission, Region IV, 1600 East Lamar Blvd., Arlington, Texas 76011-4511, and emailed to R4Enforcement@nrc.gov within 30 days of the date of this letter. If an adequate response is not received within the time specified or an extension of time has not been granted by the NRC, the NRC will proceed with its enforcement decision or schedule a PEC.

If you choose to request a PEC, the conference will afford you the opportunity to provide your perspective on these matters and any other information that you believe the NRC should take into consideration before making an enforcement decision. The decision to hold a PEC does not mean that the NRC has determined that a violation has occurred or that enforcement action will be taken. This conference would be conducted to obtain information to assist the NRC in making an enforcement decision. The topics discussed during the conference may include information to determine whether a violation occurred, information to determine the significance of a violation, information related to the identification of a violation, and information related to any corrective actions taken or planned.

In lieu of a PEC, you may also request ADR with the NRC in an attempt to resolve this issue. Alternative dispute resolution is a general term encompassing various techniques for resolving conflicts using a neutral third party. The technique that the NRC has decided to employ is mediation. Mediation is a voluntary, informal process in which a trained neutral (the “mediator”) works with parties to help them reach resolution. If the parties agree to use ADR, they select a mutually agreeable neutral mediator who has no stake in the outcome and no power to make decisions. Mediation gives parties an opportunity to discuss issues, clear up misunderstandings, be creative, find areas of agreement, and reach a final resolution of the issues. Additional information concerning the NRC's program can be obtained at http://www.nrc.gov/about-nrc/regulatory/enforcement/adr.html. The Institute on Conflict Resolution (ICR) at Cornell University has agreed to facilitate the NRC's program as a neutral third party. Please contact ICR at (877) 733-9415 within 10 days of the date of this letter if you are interested in pursuing resolution of this issue through ADR.

In addition, please be advised that the number and characterization of apparent violations described in the enclosed inspection report may change as a result of further NRC review. You will be advised by separate correspondence of the results of our deliberations on this matter.

In accordance with 10 CFR 2.390 of the NRC’s “Agency Rules of Practice and Procedure,” a copy of this letter, its enclosure, and your response, if you choose to provide one, will be made available electronically for public inspection in the NRC Public Document Room and from the NRC’s Agencywide Documents Access and Management System (ADAMS), accessible from the NRC website at http://www.nrc.gov/reading-rm/adams.html. To the extent possible, your response should not include any personal privacy or proprietary information so that it can be made available to the public without redaction.

If you have any questions concerning this matter, please contact Shiattin Makor of my staff at (817) 200-1507.

Sincerely,

 Signed by Patricia Vossmar on 09/16/26

Patricia J. Vossmar, Director
R4 Division of Reactor Safety

Docket No. 05000458
License No. NPF-47

Enclosures:
1. Factual Summary
2. NRC Inspection Report 05000458/2026092

cc w/ encl: Granicus Communications

FACTUAL SUMMARY
OFFICE OF INVESTIGATIONS REPORT OI-RIV-2025-0094

On December 17, 2025, the Nuclear Regulatory Commission (NRC) Office of Investigations (OI), Region IV, initiated an investigation to determine if a maintenance supervisor (a member of the critical group) employed by Entergy Operations Inc. at River Bend Station (RBS), and a contractor working at RBS (a non-critical group member) engaged in deliberate misconduct when the critical group member transferred a critical digital asset (CDA) key, along with his site access badge, to the non-critical group member. The investigation was completed on May 11, 2026.

On September 9, 2025, the maintenance supervisor checked out, to himself, a CDA key that was needed for work at the access authorization building, outside of the secure owner-controlled area (SOCA). After this work was complete, the maintenance supervisor gave the CDA key to a contractor, who was not qualified as a critical group member, for the purpose of returning the CDA key to the kiosk repository. The maintenance supervisor also gave his own access badge to the contractor, in order to scan the CDA key back into the kiosk.

During the RBS internal investigation, in a transcribed interview that was provided to the NRC, the maintenance supervisor stated that, at the time that he transferred the CDA key and access badge to the non-critical group member, he was aware of the requirements governing control of the CDA key, and that he knew the contractor was not a member of the critical group. Between 2012 and 2025, the maintenance supervisor had successfully completed site training courses multiple times which explicitly conveyed the requirements in Entergy security procedures. Specifically, EN-IT-103-07, Cyber Security Physical Access Requirements for Critical Digital Assets, states in part, “Keys that are used to control access to a CDA or an area or room that contains CDAs can only be issued by personnel who are members of the critical group to critical group members after appropriate verification… Person issued key is responsible for returning key upon completion of task performed.”

Based on the evidence developed during the investigation, it appears that the maintenance supervisor deliberately violated site procedures related to the protection of a CDA key. This appears to have caused the licensee to be in violation of 10 CFR 73.54(b)(2), which requires the implementation of a cyber security plan.

U.S. NUCLEAR REGULATORY COMMISSION
Inspection Report

Docket Number:	05000458
License Number:	NPF-47
Report Number:	05000458/2026092
Enterprise Identifier:	I-2026-092-0001
Licensee:	Entergy Operations, Inc.
Facility:	River Bend Station
Location:	St. Francisville, LA
Inspection Dates:	May 11, 2026, to August 31, 2026
Inspector:	A. Saunders, Reactor Inspector
Approved By:	Patricia J. Vossmar, Director R4 Division of Reactor Safety

SUMMARY

The U.S. Nuclear Regulatory Commission (NRC) continued monitoring the licensee's performance by conducting an NRC inspection at River Bend Station, in accordance with the Reactor Oversight Process. The Reactor Oversight Process is the NRC's program for overseeing the safe operation of commercial nuclear power reactors. Refer to https://www.nrc.gov/reactors/operating/oversight.html for more information.

List of Findings and Violations

Failure to Fully Implement Cyber Security Program Requirements			
Cornerstone	Severity	Cross-Cutting Aspect	Report Section
Not Applicable	Apparent Violation AV 05000458/2026092-01 Open EAF-RIV-2026-0049	Not Applicable	Not Applicable
The NRC identified an apparent violation of 10 CFR 73.54(b)(2), Renewed Operating License No. NPF-47 Condition 2.E, and the Cyber Security Plan. Specifically, a supervisor that was a critical group member failed to maintain custody and control of a critical digital asset (CDA) key when it was transferred to a non-critical group contractor to return the key back into the protected area (PA).			

Additional Tracking Items

None.

INSPECTION RESULTS

Failure to Fully Implement Cyber Security Program Requirements			
Cornerstone	Severity	Cross-Cutting Aspect	Report Section
Not Applicable	Apparent Violation AV 05000458/2026092-01 Open EAF-RIV-2026-0049	Not Applicable	Not Applicable

The NRC identified an apparent violation of 10 CFR 73.54(b)(2), Renewed Operating License No. NPF-47 Condition 2.E, and the Cyber Security Plan. Specifically, a supervisor that was a critical group member failed to maintain custody and control of a critical digital asset (CDA) key when it was transferred to a non-critical group contractor to return the key back into the protected area (PA).

Description: On September 9, 2025, at River Bend Station (RBS), a maintenance supervisor transferred a CDA key and his site-access badge to a non-critical group contractor for the purpose of returning the CDA key to the designated kiosk. This action was identified by the licensee and is in violation of cybersecurity plan requirements identified in appendix A, section 4.10, “Policies and Implementing Procedures;” Appendix E, Section 5, “Physical Protection;” and implemented by procedure EN-IT-103-07, “Cyber Security Physical Access Requirements for Critical Digital Assets,” Revision 9. This procedure implements the cyber security plan control and together the procedures prohibit the transfer of CDA keys to unauthorized individuals.

The incident was initially observed by IT personnel, who later confirmed through badge transaction logs and photo verification that the maintenance supervisor transferred the badge to return the CDA key. When questioned, the maintenance supervisor admitted to knowingly transferring the badge and key, citing that time constraints and familiarity with the contractor influenced their decision.

The licensee conducted an internal investigation and substantiated willful violations by both individuals. Both individuals were terminated from their respective organizations. The licensee initiated corrective actions, including a sitewide standdown on cyber security key control, an organizational and programmatic evaluation, and a review of key control practices across other sites.

Cyber Security Plan (CSP) Appendix A, Section 4.10 requires, in part, that policies and implementing procedures are developed to meet the implemented cyber security control’s objectives provided in Appendices D and E of the cyber security plan. The program policies and implementing procedures are documented, developed, reviewed, approved, issued, used, and revised as described in Section 4 of this Plan. Because the cyber key was issued for use on CDAs installed outside the protected area, the cyber security controls in Appendix E, section 5, “Physical Protection,” also apply.

The CSP controls in Appendix A, Section 4.10 and Appendix E, section 5 are implemented in part by procedure EN-IT-103-07, “Cyber Security Physical Access Requirements for Critical

Digital Assets," Revision 9. Step 4.8 of this procedure requires, in part that all personnel are responsible to maintain custody control of media, keys, and passwords. The person who issued the key is responsible for returning key upon completion of the task performed. Step 5.1.8 also stipulates that keys cannot be transferred from one critical group member to another critical group member. Step 5.3.4 specifies that custody and control of CDA keys must be maintained by critical group members.

Despite the guidance, when the licensee failed to maintain custody and control of the CDA key, they failed to comply with the requirements of 10 CFR 73.54 by not properly implementing the onsite cyber security program as mandated by commission regulations, including the development and use of security plans and written implementing procedures.

License Condition 2.E requires, in part, that the licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan, including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p).

Contrary to the above, on September 9, 2025, the licensee failed to fully implement the requirements of their cyber security plan and plant procedures. Specifically, a supervisor that was a critical group member failed to maintain custody and control of a CDA key when he transferred it to a non-critical group so the contractor could return the CDA key.

Corrective Actions: The licensee generated a condition report and performed a standdown for all personnel on proper handling of CDA keys.

Corrective Action References: CR-RBS-2025-05032, CR-RBS-2025-05039, CR-RBS-2025-00753

Enforcement: The ROP's significance determination process does not specifically consider willfulness in its assessment of licensee performance. Therefore, it is necessary to address this violation which involves willfulness using traditional enforcement to adequately deter non-compliance.

Severity: The severity of this apparent violation will be finalized in accordance with the Enforcement Policy pending a final enforcement determination. The violation was assessed per the "NRC Enforcement Policy," dated February 24, 2026, Section 2.2.1.d, "Whether the violation involved willfulness," states: "Willful violations are of particular concern because the NRC's regulatory program is based on licensees and their contractors, employees, and agents acting with integrity and communicating with candor. The Commission cannot tolerate willful violations. Therefore, a violation may be considered more significant than the underlying non-compliance if it includes indications of willfulness. Violations with willful aspects will typically be considered for escalated enforcement. The term "willfulness" as used in this Policy refers to conduct involving either a careless disregard for requirements or a deliberate violation of requirements or falsification of information."

Violation:
Renewed Facility Operating License No. 47, License Condition 2.E requires, in part, that the licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan, including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p).

Title 10 CFR 73.54(b)(2) requires, in part, that the licensee establish, implement, and maintain a cyber security program for the protection of safety, security, and emergency preparedness (EP) assets from cyberattacks.

Cyber Security Plan Appendix A, Section 4.10, "Policies and Implementing procedures," requires, in part, that program policies and implementing procedures are used as described in Section 4 of the Plan; Appendix E, Section 5, "Physical Protection," requires, in part, that for CDAs located outside the protected area, the licensee ensures only qualified and authorized individuals obtain access to CDAs, and controls physical access to the CDAs independent of the physical access controls for the facility.

Section 4.8 of Entergy procedure EN-IT-103-07, "Cyber Security Physical Access Requirements for Critical Digital Assets," Revision 9, an implementing procedure of the Cyber Security Plan, states in part that all personnel are responsible for maintaining custody control of media, keys, and passwords (pins) while on site (owner-controlled area or EP offsite locations), and that the person issued the key is responsible for returning the key upon completion of task performed. Section 5.1.8 states that keys cannot be transferred from one critical group member to another critical group member like media, and that the person issued the key is responsible for returning key upon completion of task performed. Section 5.3.4 states that custody and control of CDA keys must be maintained by critical group members escorting non-critical group members inside and outside of the PA.

Contrary to the above, on September 9, 2025, the licensee failed to fully implement the requirements of their cyber security plan and plant procedures. Specifically, a supervisor that was a critical group member failed to maintain custody and control of a CDA key when he transferred it to a non-critical group contractor so that the contractor could return the CDA key.

Enforcement Action: This violation is being treated as an apparent violation pending a final significance (enforcement) determination.

EXIT MEETINGS AND DEBRIEFS

The inspectors verified no proprietary information was retained or documented in this report.

- On August 31, 2026, the inspectors presented the NRC inspection results to Phil Hansett, Site Vice President, and other members of the licensee staff.

Phil Hansett
SUBJECT: RIVER BEND STATION - NRC INSPECTION REPORT 05000458/2026092 AND INVESTIGATION REPORT OI-RIV-2025-0094 DATED: September 16, 2026

DISTRIBUTION:
J Monninger
G Warnick
P Vossmar
J Josey
D Cylkowski
E Stamm
T Smith
A Moreno
R Alexander
D Dodson
C Wynar
L Day
S Schwind
A Roberts
C Alldredge
L Wilkins
E Powell
S Makor
J Groom
A Saunders
D Furst
P McKenna
S Graves
S Walker
S Lewman
I Curry
J Schussler