



Davis-Besse Nuclear Power Station

Terry J. Brown
Site Vice President
5501 N. State Route 2
Oak Harbor, OH 43449
Office: 419.321.7676

L-26-184
October 13, 2026

10 CFR 50.54(p)(2)

ATTN: Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Davis-Besse Nuclear Power Station, Unit 1
Docket Number 50-346, License Number NPF-3
Davis-Besse Nuclear Power Station Cyber Security Plan (Revision 3)

This letter forwards Revision 3 of the Davis-Besse Nuclear Power Station (DBNPS) Cyber Security Plan (CSP), which was effective on August 19, 2026. The Attachment provides a summary of the Revision 3 CSP changes. These changes were reviewed and determined not to decrease the effectiveness of the DBNPS CSP. Accordingly, this revision is being submitted in accordance with the provisions of 10 CFR 50.54(p)(2).

The Enclosure containing the revision of the DBNPS CSP contains Security Related Information and should be withheld from public disclosure under the provisions of 10 CFR 2.390.

There are no regulatory commitments contained in this letter. If there are any questions or if additional information is required, please contact Ms. Lillie Winckowski, Senior Manager, Technology Services, at (419) 321-8584.

Sincerely,

A handwritten signature in black ink, appearing to read "Terry J. Brown", written over a horizontal line.

Terry J. Brown

CDA

Attachment: Summary of DBNPS CSP Revision 3 Changes

Enclosure: Davis-Besse Nuclear Power Station Cyber Security Plan Revision 3

~~THE ENCLOSURE TO THIS LETTER CONTAINS SECURITY RELATED INFORMATION.~~
~~WITHHOLD UNDER 10 CFR 2.390. UPON THE REMOVAL OF THE ENCLOSURE TO THIS~~
~~LETTER, THIS LETTER IS UNCONTROLLED.~~

Davis-Besse Nuclear Power Station, Unit 1

L-26-184

Page 2 of 2

cc: NRC Region III Administrator
NRC Resident Inspector (w/o Enclosure)
NRR Project Manager (w/o Enclosure)
Utility Radiological Safety Board (w/o Enclosure)

~~THE ENCLOSURE TO THIS LETTER CONTAINS SECURITY RELATED INFORMATION.
WITHHOLD UNDER 10 CFR 2.390. UPON THE REMOVAL OF THE ENCLOSURE TO THIS
LETTER, THIS LETTER IS UNCONTROLLED.~~

Attachment
L-26-184

Summary of DBNPS CSP Revision 3 Changes
Page 1 of 7

The following summarizes the Davis-Besse Nuclear Power Station (DBNPS) Cyber Security Plan (CSP) Revision 3 Changes made effective August 19, 2026

DESCRIPTION OF THE CHANGE(s):

1. Table of Contents, the title of Section 4.10, was changed from “Policies and Implementing Procedures” to “Policy, Implementing Procedures and Business Practices.”
2. Throughout the document, references to “policies and procedures” are changed to “policy, procedures and business practices.”
3. Throughout the document terms such as the following are capitalized to identify them as proper nouns with a specific meaning relative to the CSP or nuclear in general: Safety Related, Important to Safety, Emergency Preparedness, Cyber Security Program, Physical Protection Program, Defense in Depth, Design Basis Threat, Cyber Security Event Notifications, Nuclear Power Plant Operations, Engineering and Nuclear Safety.
4. Throughout the document references to NEI 08-09, Revision 6 Addendum 1, are changed to NEI 08-09, Revision 7.
5. Throughout the document common abbreviations such as the following are spelled out upon first mention and in subsequent occurrences may only use the abbreviation: (HVAC) as an abbreviation following heating, ventilation, and air conditioning, (CSIRT) as an abbreviation for cyber security incident response team, (CAP) as an abbreviation for Corrective Action Program, (SSEP) as an abbreviation for Safety, Security and Emergency Preparedness.
6. Section 2.1 eliminates the following paragraph:

Within the scope of NRC’s cyber security rule at 10 CFR 73.54, systems or equipment that perform important to safety functions include structures, systems, and components (SSCs) in the Balance of Plant (BOP) that could directly or indirectly affect reactivity at a nuclear power plant and could result in an unplanned reactor shutdown or transient. Additionally, these SSCs are under the licensee’s control and include electrical distribution equipment out to the first inter-tie with the offsite distribution system.

This is replaced by a definition of BOP that is now included in the Glossary.

~~THE ENCLOSURE TO THIS LETTER CONTAINS SECURITY RELATED INFORMATION.
WITHHOLD UNDER 10 CFR 2.390. UPON THE REMOVAL OF THE ENCLOSURE TO THIS
LETTER, THIS LETTER IS UNCONTROLLED.~~

7. Section 3.1.5, 1st paragraph removes “to the extent required to perform assessments in accordance with Section 3.1.6 (e.g. the data gathered for direct and indirect CDAs may differ)” from a statement identifying that CSAT conducts tabletop review and validation activities.
8. Section 3.1.6, 3rd paragraph deletes “When a cyber security control is determined to have an adverse effect” which was repeated from the previous sentence and adds “OR when alternate controls are implemented that mitigate the consequence(s) of the threat/attack vector associated with the control.”
9. Section 3.1.6, 3rd paragraph adds the word “Alternate” to the sentence “Controls are used to mitigate the lack of the security control for the CDA per the process described in this section”.
10. Section 3.1.6, 4th paragraph changes “Revision 6” to “Revision 7” when referencing NEI 13-10 Cyber Security Control Assessments.
11. Section 3.1.7 is a new section that adds the following:

The cyber security controls in this plan, in combination with the security controls prescribed by 10 CFR 73.55(b) may implement more than one barrier against exploitation of a cyber attack threat vector.

As noted at the beginning of Section 3, implementing Appendix D and E cyber security controls provides high-assurance of adequate protection of CDAs associated with SSEP functions, creating a substantive Defense-in-Depth Cyber Security Program with significant layers of protection. This comprehensive approach to implementing technical, operational, and programmatic security controls creates a robust cyber defensive posture such that the degradation of a subset of security control(s) does not inherently reduce margin of adequate protection of the SSEP function.

In cases where there is degradation or failure of specific cyber security control, margin may exist. Before making that determination, the impact of degradation or failure must be assessed to determine the effect(s) on Defense-in-Depth protection. The licensee must also assess the CDA, the relevant attack vectors, and the intent of the degraded cyber control in accordance with the process described in Section 3.1.6.

If protections still exist, such that the degradation or failure of the CDA controls would not result in a substantive increase of an adversary's ability to successfully exploit the threat / attack vector(s) that the control is intended to protect, then the effect(s) of the degradation or failure on Defense-in-Depth would be reduced. When a degradation or failure of cyber security control is identified, it must be entered into the licensee's Corrective Action Program for remediation.

~~THE ENCLOSURE TO THIS LETTER CONTAINS SECURITY RELATED INFORMATION.
WITHHOLD UNDER 10 CFR 2.390. UPON THE REMOVAL OF THE ENCLOSURE TO THIS
LETTER, THIS LETTER IS UNCONTROLLED.~~

12. Section 4.3 4th paragraph, bullet 1, changes the words “layers” and “layer” to “levels” and “Level”.
13. Section 4.3, 4th paragraph, bullet 4, removes “air gaps” from the examples of deterministic devices that are identified in parenthesis and adds “or air gap” outside of the parenthesis.
14. Section 4.3, bullet 5, sub bullet 1, removes “air gap” from a list of examples of deterministic devices.
15. Section 4.3, bullet 6 adds the following:

Information flow directly from level 4 to level 2 is implemented through the use of one or more deterministic devices (e.g., data diode, one-way serial device) that isolate CDAs in Level 4.
16. Section 4.4.2 adds the word “site” before “CAP” to clarify which Corrective Action Program shall be used to track adverse conditions.
17. Section 4.4.3.1, 1st paragraph replaces:

Reviews of the cyber security program and controls include but are not limited to periodic audits of the physical security program, security plans, implementing procedures, cyber security programs; safety/security interface activities; the testing, maintenance, and calibration program as it relates to cyber security; and feedback from the NRC and local, state and federal law enforcement authorities.

These reviews are coordinated by the Corporate Cyber Security Program.

With:

Reviews of the Cyber Security Program and controls include, but are not limited to, periodic audits as a component of the Physical Security Program and feedback from the NRC inspections and other assessments.
18. Section 4.4.3.1, 2nd paragraph replaces:

The effectiveness evaluation provides information for cyber security decision makers about the results of previous policy and acquisition decisions. These measures:

With the following:

The Effectiveness Analysis should provide information for evaluating corrective actions implemented pertaining to the Cyber Security Program and the enrollment of newly installed plant equipment in the Cyber Security Program. Key information in these areas should support the ongoing analysis regarding

~~THE ENCLOSURE TO THIS LETTER CONTAINS SECURITY RELATED INFORMATION.
WITHHOLD UNDER 10 CFR 2.390. UPON THE REMOVAL OF THE ENCLOSURE TO THIS
LETTER, THIS LETTER IS UNCONTROLLED.~~

the effectiveness of the implemented program. The Effectiveness Analysis should also do the following:

19. Section 4.4.3.1, 2nd paragraph, 3rd and 4th bullets replace:

- Assist in ascertaining whether specific cyber security controls are functioning and are helping facilitate corrective action prioritization; and
- Require combining the Cyber Security Program activities data with the data obtained from automated monitoring and evaluation tools in a manner that can be tied to cyber security control implementation.

With the following:

- Facilitate corrective action prioritization; and
- Provide reviews for both programmatic activities and data obtained from automated monitoring in order to present an overall picture of program health.

20. Section 4.4.3.2 2nd paragraph, eliminates the requirement to document all discovered vulnerabilities in CAP and replaces it with a requirement to keep records of vulnerability reviews and to document those vulnerabilities that require mitigation in CAP.

21. Section 4.4.3.2 2nd paragraph, last sentence:

Information obtained from the vulnerability scanning process is shared with appropriate personnel to ensure that similar vulnerabilities that may impact interconnected or similar CDA(s) are understood, evaluated and mitigated.

Is replaced with:

Vulnerabilities that pose a risk to SSEP functions are mitigated when the evaluation concludes remediation is required to maintain adequate Defense-in-Depth.

22. Section 4.10 adds that the senior nuclear management responsible for the management and implementation of the program is Vice-President Nuclear Site.

23. Section 4.11 includes several changes to identify the roles and responsibilities that are specific to the Vistra Cyber Security Program.

- a. Changes the role from Cyber Security Program Sponsor to Cyber Security Station Sponsor and adds "DBNPS" to precede several references to the Cyber Security Program.

~~THE ENCLOSURE TO THIS LETTER CONTAINS SECURITY RELATED INFORMATION.
WITHHOLD UNDER 10 CFR 2.390. UPON THE REMOVAL OF THE ENCLOSURE TO THIS
LETTER, THIS LETTER IS UNCONTROLLED.~~

- b. Adds the role of Cyber Security Corporate Sponsor who has corporate level responsibility for the Cyber Security Program and ensuring adequate resources are available to support the program.
 - c. Adds the role of Cyber Security Compliance Program Manager that functions as the Fleet Cyber Security Program Manager.
 - d. Adds the role of Cyber Security Generation Security Manager.
 - e. Adds the role of Site Cyber Security Program Manager.
 - f. Adds the following responsibility to the role of Cyber Security Specialist: Conduct cyber security audits, network scans, and penetration tests against CDAs as necessary.
 - g. Changes Cyber Security Incident Response Team (CSIRT) reference from “DBNPS” incident response procedures to “site” incident response procedures.
24. Section 4.13, 2nd paragraph deletes identification of records to be retained by identifying “examples of records or supporting technical documentation” and replaces the examples with a specific list of records or reference to the section in which the records are generated.
25. Section 4.13, 2nd paragraph adds that the period for retaining superseded records is at least 3 years after the records have been superseded.
26. Section 4.13 is changed to provide clarifications for retention of CDA audit records. Specific changes are identified below:
- a. Both manual audit records and audit records where a central server is employed shall be retained for no less than 12 months.
 - b. A description of auditable events is replaced by a specific reference to sections (Appendix D, 2.3 and Appendix E) that generate audit records.
 - c. Reference to “electronic and non-electronic audit records” is changed to “digital and non-digital audit records.”
27. Section 4.13 identifies that audit data is not required to be maintained under the QA Records Program.
28. Section 4.13 replaces a general reference to retain training records to document personnel qualifications with a requirement to document and maintain Cyber Security Training Records for 3 years.
29. Attachment 1, Glossary is modified to include additional definitions from NEI 08-09 Rev. 7 and also updates a reference from RG 5.71 Rev. 0 to RG 5.71 Rev.1.

~~THE ENCLOSURE TO THIS LETTER CONTAINS SECURITY RELATED INFORMATION.
WITHHOLD UNDER 10 CFR 2.390. UPON THE REMOVAL OF THE ENCLOSURE TO THIS
LETTER, THIS LETTER IS UNCONTROLLED.~~

30. Appendix D 1.9 Previous Logon Notification is deleted.

31. Appendix D 1.11 Supervision and Review – Access Control is deleted.

32. Appendix D 1.16 Open/Insecure Protocol Restrictions changes:

Documents and takes additional precautions to protect networks and bus communications from unauthorized access where protocols lack security controls.

To the following:

If a protocol lacks security controls to protect networks and bus communications from unauthorized access, take the following additional precautions:

33. Appendix D 1.17 Wireless Access Restrictions changes:

Prohibits the use of wireless technologies for CDAs associated with safety-related and important-to-safety functions.

To the following:

The use of wireless communications for the control of CDAs associated with SR and ITS functions is prohibited.

34. Appendix D 1.17 Wireless Access Restrictions adds the following note:

[Note: “associated with” does not preclude the use of wireless technology for the use of monitoring nor data collection. The prohibition is directed at the use of wireless technology for manipulation (i.e. control) of the system safety functions. The use of wireless technology will not be solely relied upon for making operational or safety decisions. Licensees must also analyze the impact of using wireless technology with safety systems to assure transmissions do not disrupt sensitive systems. An impact analysis is necessary for implementation of wireless technology for CDAs associated with safety-related and important-to-safety systems.

The use of wireless communications for monitoring CDAs associated with SR & ITS functions is permitted with the following mitigations:

- Wireless CDAs are continuously monitored for unauthorized connections to an access point (e.g., through connection to the site SIEM and IDS).
- Wireless CDAs are isolated from other wireless communication systems (e.g., business or EP system). Information may only be sent to a lower security level (e.g., to a lower level SIEM) via wired connections through a boundary device.

~~THE ENCLOSURE TO THIS LETTER CONTAINS SECURITY RELATED INFORMATION.
WITHHOLD UNDER 10 CFR 2.390. UPON THE REMOVAL OF THE ENCLOSURE TO THIS
LETTER, THIS LETTER IS UNCONTROLLED.~~

- Enforce the prohibition of changes to the wireless system to authorized personnel for making authorized changes.

35. Appendix D 1.17 Wireless Access Restrictions changes:

- Conducts scans for unauthorized wireless access points in accordance with this document and disables access points if unauthorized access points are discovered.
- Conducts scans every 31 days for unauthorized wireless access points in accessible areas in accordance with this document and disables access points if unauthorized access points are discovered.

To the following:

- Conducts and documents scans every 31 days in accessible areas to identify and disable unauthorized wireless access points capable of adversely affecting SSEP function. Examples of documentation can include heat maps showing the CDAs being scanned are within the covered area or a listing of CDAs within the scanned covered area.

36. Appendix E 7.3 Incident Response Testing and Drills changes the required periodicity from “every 12 months” to “annually.”

37. Appendix E 8.3 Contingency Training changes the required periodicity from “every 12 months” to “annually.”

38. Appendix E 10.3 Baseline Configuration changes the required periodicity from “every 92 days” to “quarterly” in two places.

39. Appendix E 10.6 Access Restrictions for Change changes the required periodicity from “every 92 days” to “quarterly.”

~~THE ENCLOSURE TO THIS LETTER CONTAINS SECURITY RELATED INFORMATION.
WITHHOLD UNDER 10 CFR 2.390. UPON THE REMOVAL OF THE ENCLOSURE TO THIS
LETTER, THIS LETTER IS UNCONTROLLED.~~