General Public Meeting Disclaimer

Participants are reminded that this meeting is public. Notice of the meeting was widely distributed. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders. Participants are also reminded to use discretion and take care not to disclose confidential information.

NPCC Outreach, Training, Events Disclaimer

Northeast Power Coordinating Council, Inc. (NPCC) is committed to providing outreach, training, and nonbinding guidance to industry stakeholders on important industry topics. Subject Matter Experts (SMEs) from NPCC's organizational groups and the industry may develop materials, including presentations, provided as part of the event. The views expressed in the event materials are those of the SMEs and do not necessarily express the opinions and views of NPCC.

Antitrust Compliance Guidelines

It is NPCC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. The antitrust laws make it important that meeting participants avoid discussion of topics that could result in charges of anti-competitive behavior, including: restraint of trade and conspiracies to monopolize, unfair or deceptive business acts or practices, price discrimination, division of markets, allocation of production, imposition of boycotts, exclusive dealing arrangements, and any other activity that unreasonably restrains competition.

It is the responsibility of every NPCC participant and employee who may in any way affect NPCC's compliance with the antitrust laws to carry out this commitment.

Participants in NPCC activities (including those participating in its committees, task forces and subgroups) should refrain from discussing the following throughout any meeting or during any breaks (including NPCC meetings, conference calls and informal discussions):

- Industry-related topics considered sensitive or market intelligence in nature that are outside of their committee's scope or assignment, or the published agenda for the meeting;
- Their company's prices for products or services, or prices charged by their competitors;
- Costs, discounts, terms of sale, profit margins or anything else that might affect prices;
- The resale prices their customers should charge for products they sell them;
- Allocating markets, customers, territories or products with their competitors;
- Limiting production;
- Whether or not to deal with any company; and
- Any competitively sensitive information concerning their company or a competitor.

Any decisions or actions by NPCC as a result of such meetings will only be taken in the interest of promoting and maintaining the reliability and adequacy of the bulk power system.

Any NPCC meeting participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NPCC's antitrust compliance policy is implicated in any situation should call NPCC's General Counsel and Corporate Secretary, Mr. Damase Hebert at (646) 737-2335 or dhebert@npcc.org.

Source: NPCC_antitrust-compliance-guidelines.pdf

Webinar Housekeeping

Recording: This webinar is being recorded. A link to the recording will be shared with all registrants after the session, so you can revisit the content or share it with colleagues.

Audio: All participants are muted by default to minimize background noise. If you experience any audio issues, try refreshing your browser or checking your device settings.

Q&A: We encourage your questions! Please use the Q&A box at the top of your screen to submit questions at any time. We'll address as many as we can during the Q&A portion at the end.

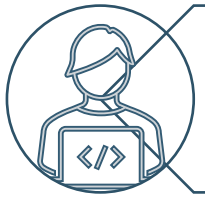
CIP-003-8 R2 in Practice

Emily Stuetzle
Manager, CIP Compliance

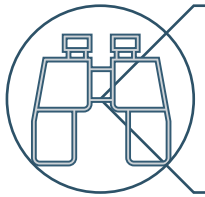
David Guerra
Senior CIP Analyst

NPCC, Inc.

Agenda



CIP-003-8 R2



Looking Ahead

Resources

Q&A

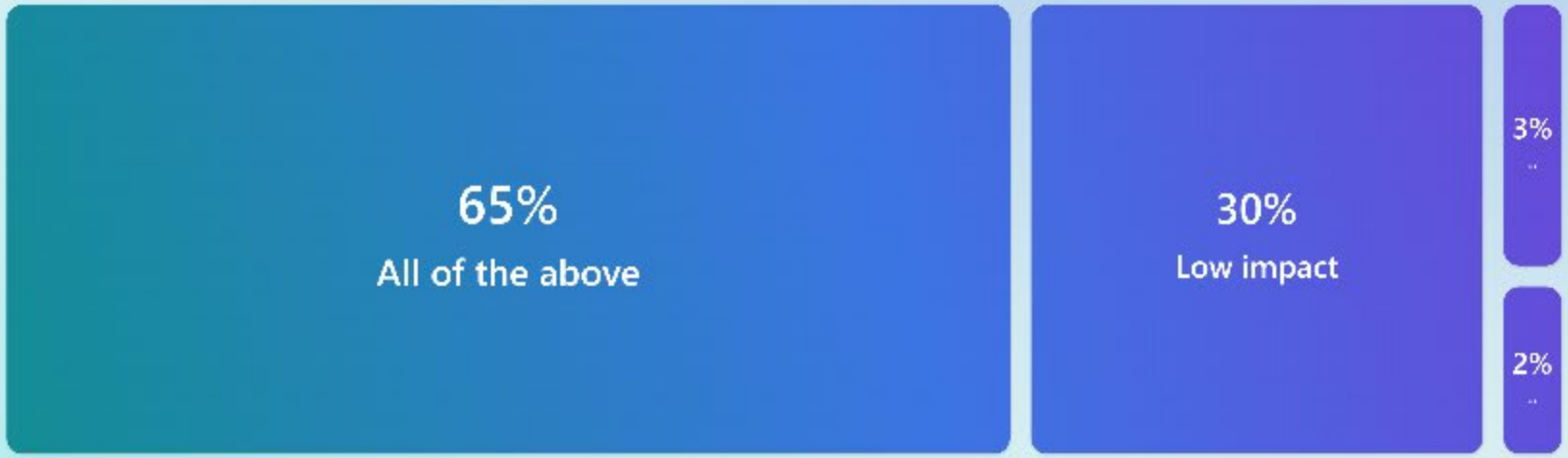
Scan the QR or use link to join

https://forms.office.com/r/NMxnq8KPKK

Copy link

64 responses submitted

Which BES Cyber System impact level does CIP-003 apply to?



Treemap | Bar

1 of 1

CIP-003-8 Cyber Security — Security Management Controls

Purpose

- To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

CIP-003-8 R2 (Cont.)

Applicable Systems

- Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.

CIP-003-8 R2 Documented Processes

The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

CIP-003-8 R2 (Cont.)

Attachment 1

Section One	Section Two	Section Three	Section Four	Section Five
• Cyber Security Awareness	• Physical Security Controls	• Electronic Access Controls	• Cyber Security Incident Response	• Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation

Section One - Cyber Security Awareness

Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices)

Section One - Cyber Security Awareness (Cont.)

Examples of Evidence

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

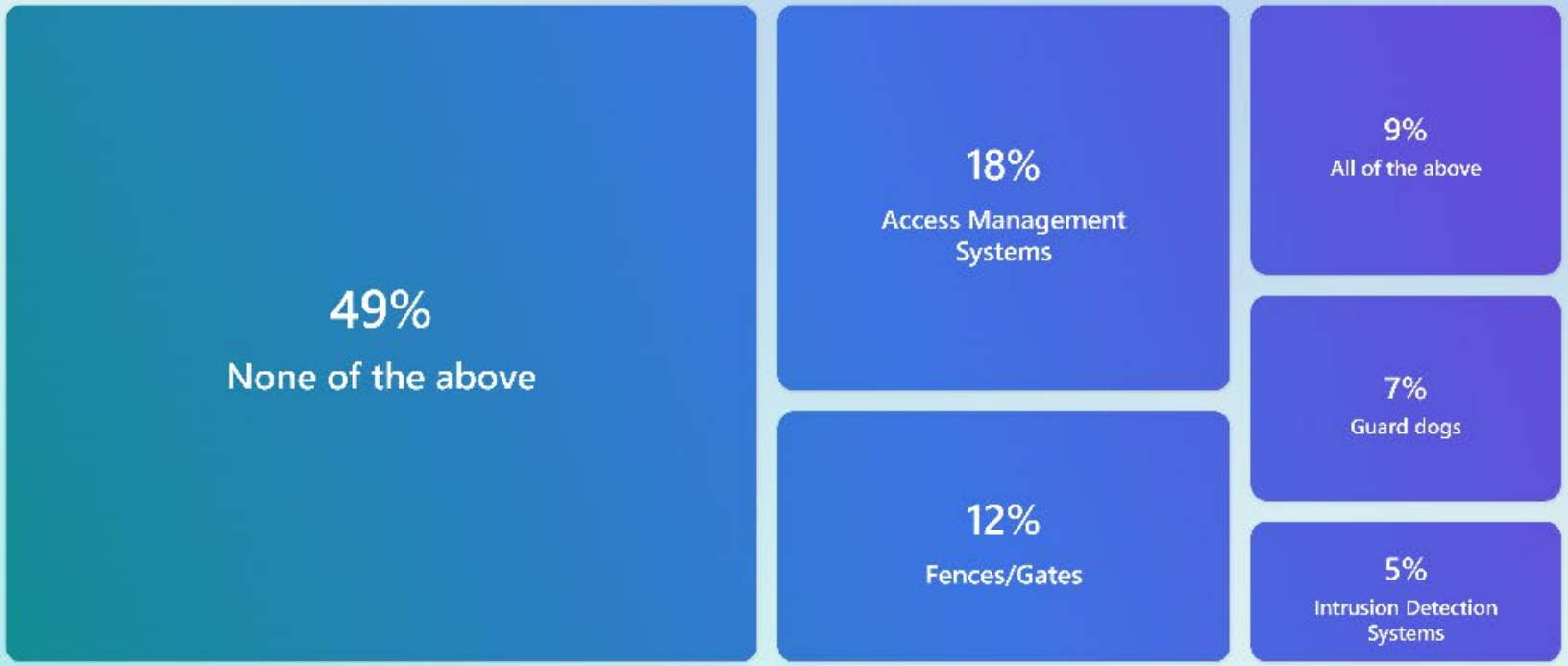
Scan the QR or use link to join

https://forms.office.com/r/Nt6DJ6DjsQ

Copy link

57 responses submitted

Section 2: Which physical security controls are required to comply with CIP-003-8 Attachment 1 Section 2?



Treemap | Bar

1 of 1

Section Two - Physical Security Controls

Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section Two - Physical Security Controls (Cont.)

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access.

Scan the QR or use link to join

https://forms.office.com/r/5bkcmRepKe

Copy link

50 responses submitted

Section 3: Which of these types of network connectivity is excluded from Attachment 1 Section 3?

Treemap | Bar

1 of 1

Section Three - Electronic Access Controls

- Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:
  - between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);
  - using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and
  - not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR61850-90-5 R-GOOSE).
- Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section Three - Electronic Access Controls (Cont.)

Examples of Evidence

- Representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s).
- Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).
- Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Scan the QR or use link to join

https://forms.office.com/r/eW0n4Ga4Re

Copy link

50 responses submitted

Section 4: Which are not acceptable incident response plan testing methods?

Treemap | Bar

1 of 1

Section Four - Cyber Security Incident Response

Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the CIP-003-8 - Cyber Security — Security Management Controls Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section Four - Cyber Security Incident Response (Cont.)

Examples of Evidence

- Dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the Section 4 requirements.

Scan the QR or use link to join

https://forms.office.com/r/CLZuHjYqt3

Copy link

46 responses submitted

Attachment 1 Section 5 prohibits the use of vendor managed Transient Cyber Asset(s)?

Treemap | Bar

1 of 1

Section Five - TCA and RM Malicious Code Risk Mitigation (REVISED)

5.1 TCA managed by the Responsible Entity shall implement one or more:

- Antivirus (including updates of signatures), application whitelisting, or other methods to mitigate malicious code.

5.2 TCA managed by 3rd party:

- Review malicious code prevention controls.
- Determine if any additional mitigation actions are required prior to connecting TCA.

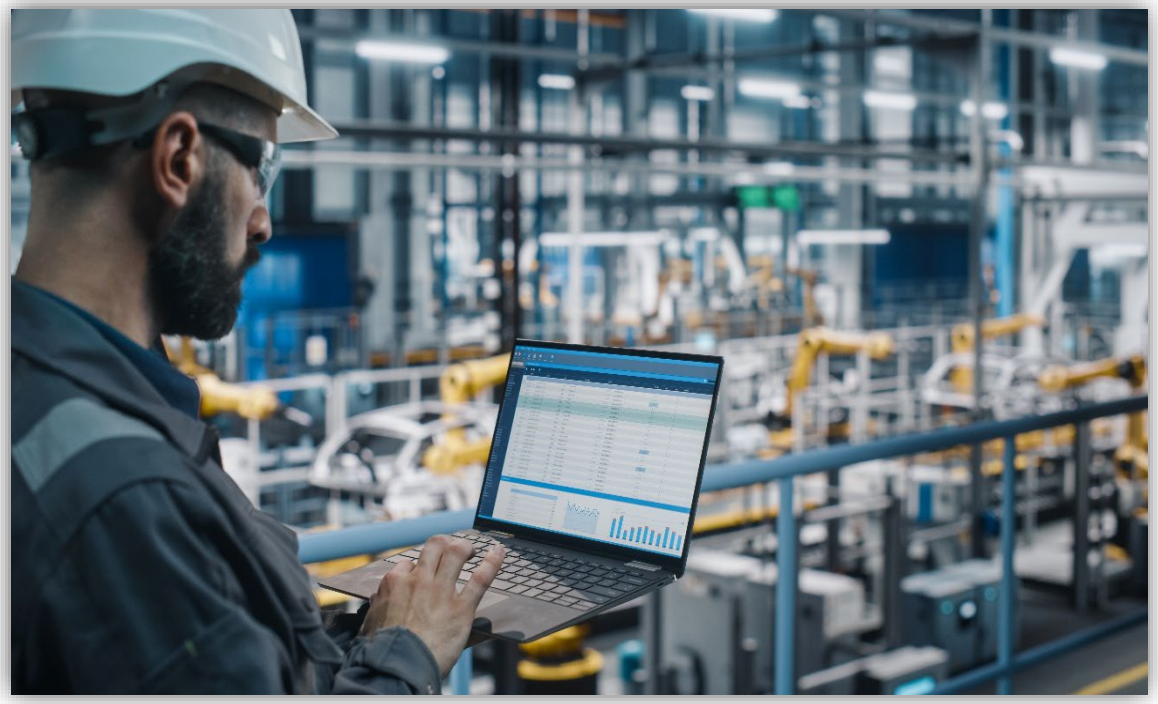
5.3 For Removable Media:

- Method to detect malicious code on removable media other than BES Cyber System.
- Mitigation of the threat of detected malicious code prior to connecting to BES Cyber System.

Section Five - TCA and RM Malicious Code Risk Mitigation (Cont.)

Examples of Evidence

- Antivirus software and processes for managing signature or pattern updates
- For third-party TCA's
  - Review of the installed antivirus update level.
- For Removable Media
  - Logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media.



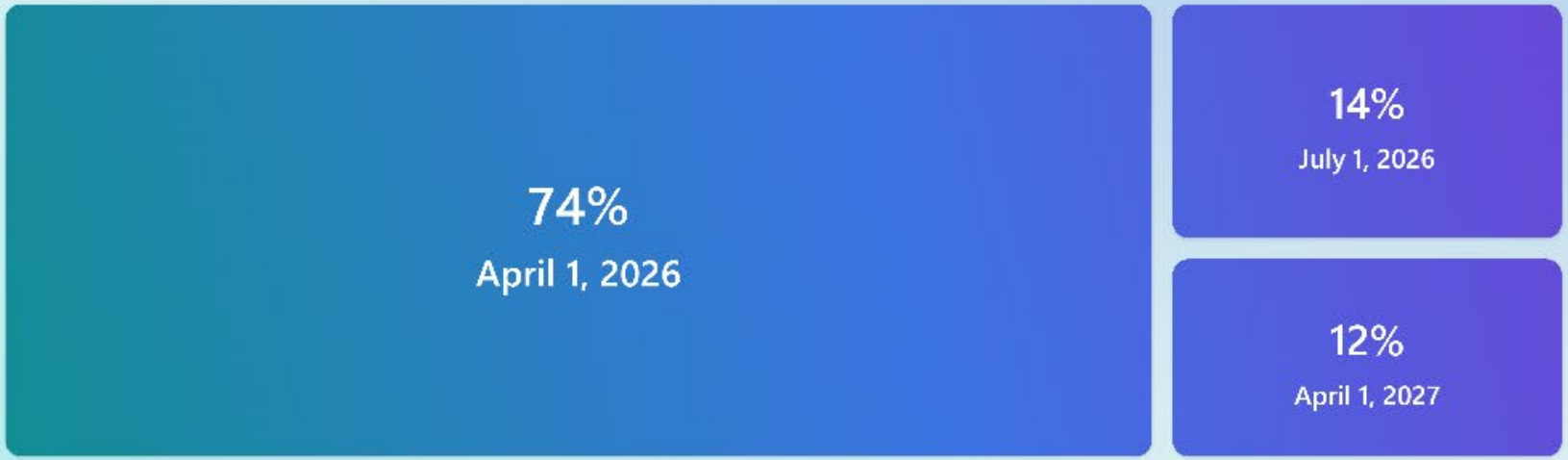
Scan the QR or use link to join

https://forms.office.com/r/Wy6mGee4JJ

Copy link

42 responses submitted

What is the effective date of CIP-003-9?



Treemap | Bar

1 of 1

Looking Ahead

CIP-003-9

- **Section Six - Vendor Electronic Remote Access Security Controls**
  - For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include: 6.1 One or more method(s) for determining vendor electronic remote access; 6.2 One or more method(s) for disabling vendor electronic remote access; and 6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Implementation Resources

NIST SP 800-53 Rev. 5

- AT-3 Role-Based Training
  - "Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Role-based training also includes policies, procedures, tools, methods, and artifacts for the security and privacy roles defined."
- AC-20 Use of External Systems
  - "Limiting authorized use recognizes circumstances where individuals using external systems may need to access organizational systems. Organizations need assurance that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems."

NIST SP 800-61 Rev. 3

- Incident Response Recommendations and Considerations for Cybersecurity Risk Management.

Sources: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile | CSRC

Questions?

Contact Us

https://www.npcc.org/contact

Upcoming NPCC Events

Reliability Forum

- August 7, 2025
- 9:00 AM – 12:00 PM (EDT)
- FERC Order 901 topics. More details to come

Fall 2025 Hybrid Compliance and Reliability Conference

- November 5 – 6, 2025
- The Gideon Putnam in Saratoga Springs
- Register