TEXAS RE

CIP-003-8 Best Practices and Challenges

Chris Mejia
CIP Cyber & Physical Security Analyst

August 19, 2025

Antitrust Admonition

Texas Reliability Entity, Inc. (Texas RE) strictly prohibits persons participating in Texas RE activities from using their participation as a forum for engaging in practices or communications that violate antitrust laws. Texas RE has approved antitrust guidelines available on its website. If you believe that antitrust laws have been violated at a Texas RE meeting, or if you have any questions about the antitrust guidelines, please contact the Texas RE General Counsel.

Notice of this meeting was posted on the Texas RE website and this meeting is being held in public. Participants should keep in mind that the listening audience may include members of the press, representatives from various governmental authorities, and industry stakeholders.

Upcoming Texas RE Events

August 26, 2025

Data Breach Response

September 9, 2025

Internal Controls

October 20, 2025

PUCT Cybersecurity Program

Upcoming Texas RE Events

September 17, 2025

Q3 MRC and Board Meetings

October 1, 2025

Winter Weatherization Workshop

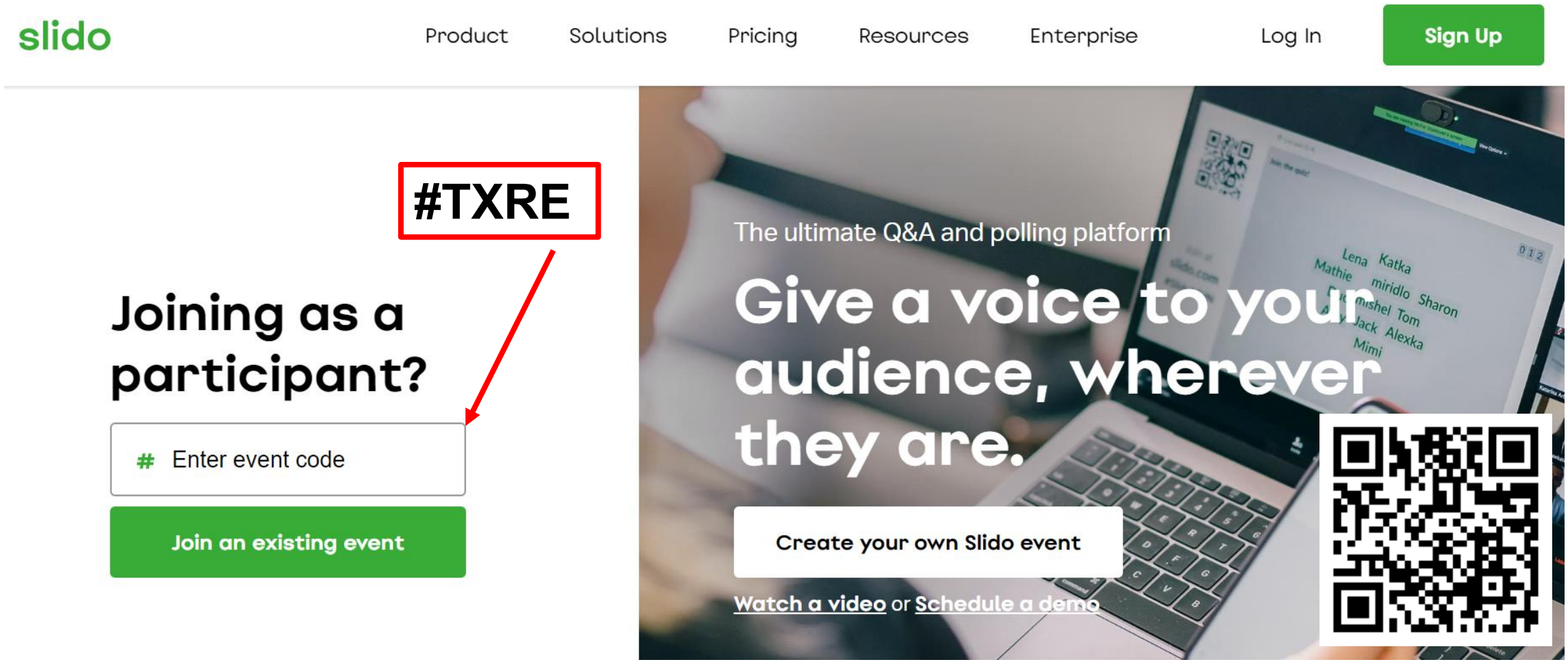
November 5, 2025

Fall Standards, Security, & Reliability Workshop

Upcoming ERO Enterprise Events

Date	Event
August 21	Reliability & Security Oversight Monthly Update (WECC)
August 26	SCOOP – Cyber Event (SERC)
September 3	Reliability in the West: Large Load System Performance (WECC)
September 8	Fall Reliability & Security Summit (RF)
September 9	System Operator Conference #3 (SERC)

Slido.com


slido
Product
Solutions
Pricing
Resources
Enterprise
Log In
Sign Up
#TXRE
Joining as a participant?
Enter event code
Join an existing event
The ultimate Q&A and polling platform
Give a voice to your audience, wherever they are.
Create your own Slido event
Watch a video or Schedule a demo

Agenda

R2

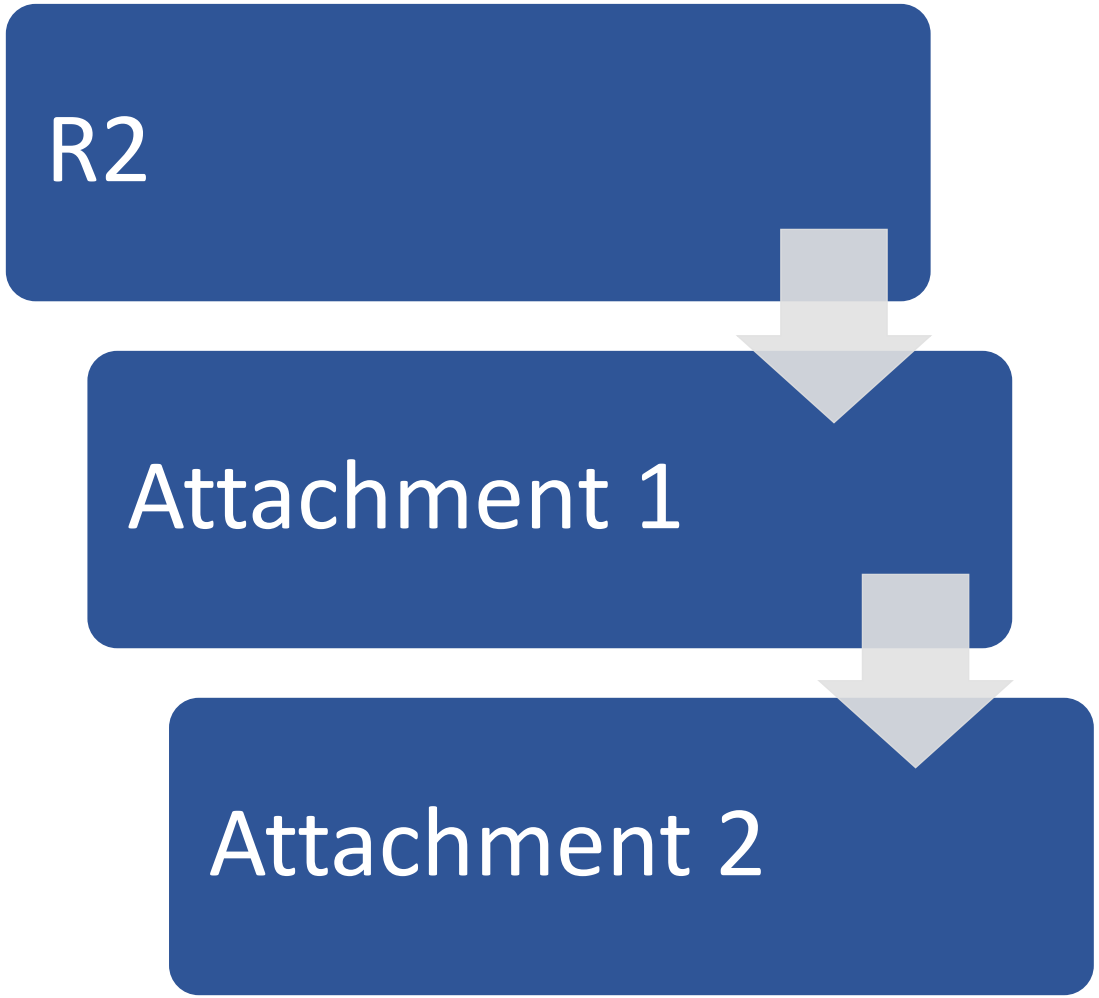
Attachment 1

What's Next?

CIP-003-8 R2

R2

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 Attachment 1

Cyber Security Plans

Section 1	Section 2	Section 3	Section 4	Section 5
Cyber Security Awareness	Physical Security Controls	Electronic Access Controls	Cyber Security Incident Response	Malicious Code Mitigation

Section 1 – Cyber Security Awareness

Reinforce every 15 calendar months

Different ways to raise awareness

Section 1 – Cyber Security Awareness

Best Practices

Direct communication

Indirect communication

Management support

Control Physical Access

Asset or locations of Bulk Electric System (BES) Cyber Systems (BCSs)

Electronic Access Controls Cyber Assets

Section 2 – Physical Security Controls

Layered Physical Access Controls

Need-Based Access

Key Management Program

Smart Locks/Badge Readers

Physical Security Perimeter (PSP) – Barbed Wire/ Fencing/Cameras

Section 3 – Electronic Access Controls

3.1 Permit only necessary inbound and outbound electronic access

- Between a low impact BCS and Cyber Asset
- Using a routable protocol when entering or leaving
- Not used for time-sensitive protection or control functions between intelligent electronic devices

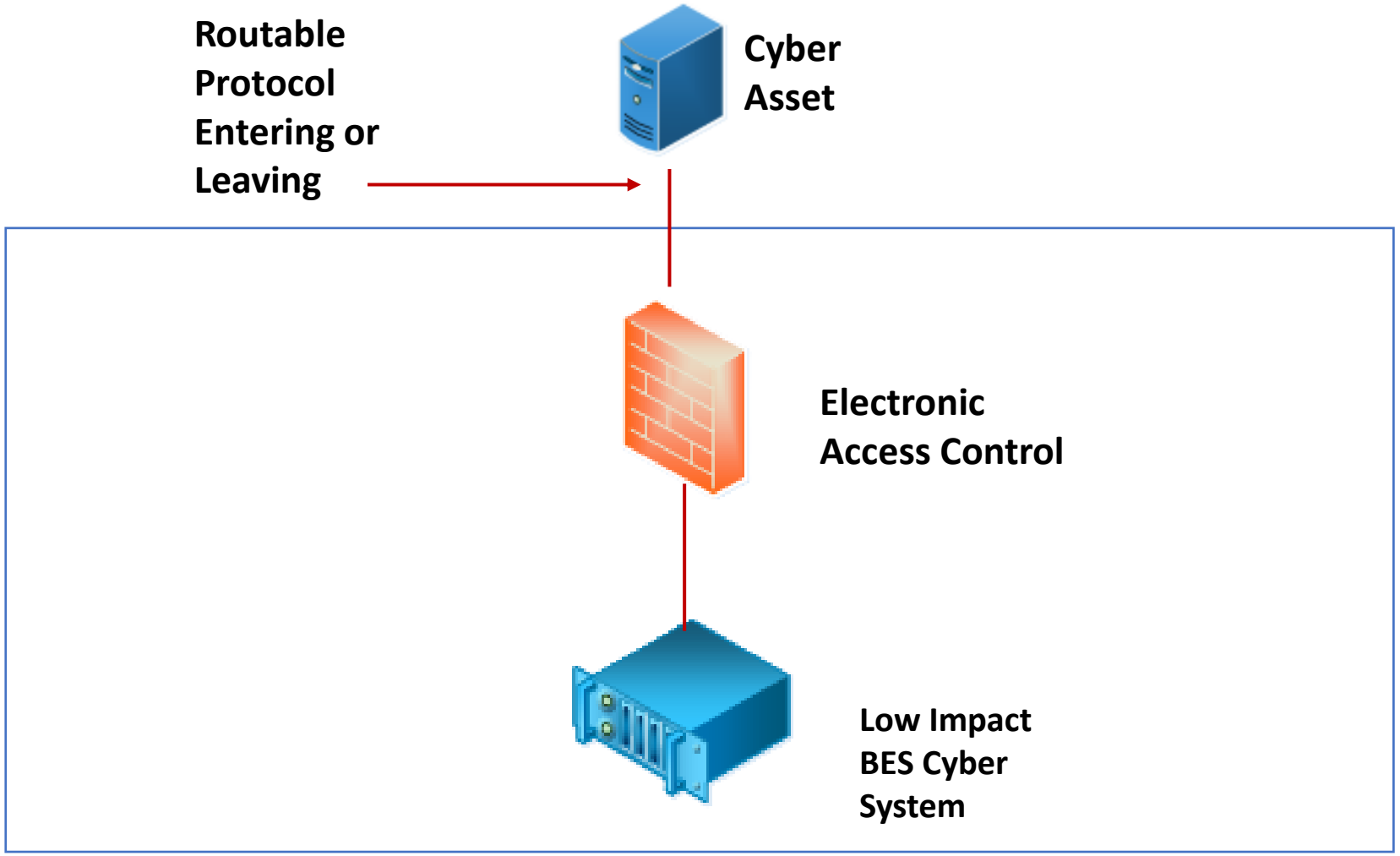
3.2 Authenticate all dial-up connectivity

Section 3 – Electronic Access Controls

Permit only what is truly necessary

Review Electronic Access Controls lists

Section 3 – Electronic Access Controls



Section 4 – Cyber Security Incident Response

Section 4 – Cyber Security Incident Response

Test on Reportable Cyber Security Incident	
Reportable Cyber Security: NERC-defined term	Test on applicable systems

Section 4 – Cyber Security Incident Response

Test Frequently

Simulate real-life Cyber Security Incidents	Participate at Grid Security Exercise (GridEx)	Involve local, state, and federal government	Incorporate lessons learned	Stress the plan

Section 5 – Transient Cyber Asset (TCA) and Removable Media (RM) Malicious Code Risk Mitigation

TCA

- TCAs managed by Responsible Entity
- TCAs managed by third party
- Additional mitigation

RM

- Method to detect malicious code
- Mitigation of the threat of detected malicious code

Section 5 – Transient Cyber Asset (TCA)

TCA Managed by Entity

Ongoing or On-demand

Antivirus software	Application whitelisting	Other method(s)

Section 5 – Transient Cyber Asset (TCA)

TCA NOT Managed by Entity

Prior to Connecting

Antivirus update level and process	Application whitelisting	Operating system and software executable only from read-only media	System hardening	Other method(s)	Mitigation actions

Section 5 – Removable Media (RM)

Removable Media

Method(s) to detect malicious code	Mitigation of the threat of detected malicious code

CIP-003-8 R2 Attachment 2

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- 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 to both:

  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and

  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

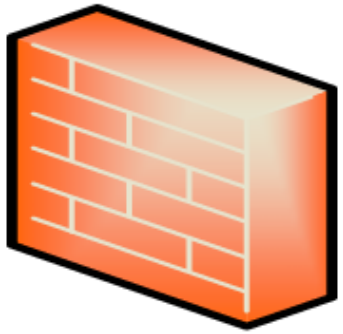
What's Next?

CIP-003-9

- Vendor Electronic Remote Access Security Controls
- April 1, 2026

Section 6 – Vendor Electronic Remote Access Security Controls

3.1 - Electronic Access Controls



Routable Protocol:

Entering or Leaving

Section 6. 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.

TEXAS RE
Ensuring electric reliability for Texans