TEXAS RE

Supply Chain

Rebekah Barber
CIP Compliance Team Lead

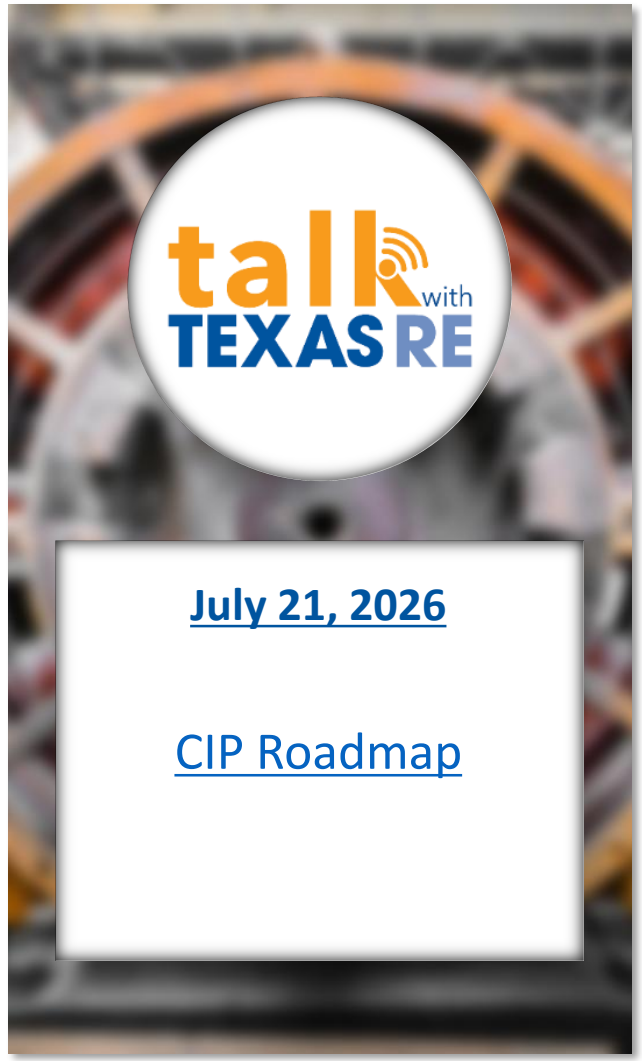
June 30, 2026

Antitrust Admonition

Because this event brings together market participants who may be viewed as actual or potential competitors, we must be mindful to conduct it in a manner that is consistent with the antitrust and competition laws. Participants should not disclose non-public, proprietary, or competitively sensitive information.

Attendees should exercise independent judgment and avoid even the appearance of discussions of agreements or concerted actions that may be viewed as restraining competition. Any questions on Texas RE's Antitrust Compliance Corporate Policy may be directed to Texas RE's General Counsel.

Upcoming Events at Texas RE



Upcoming Events at Texas RE

August 19, 2026

Winter Weatherization Workshop

September 16, 2026

Q3 MRC and Board Meetings

November 4, 2026

Fall Standards, Security, & Reliability Workshop

Upcoming ERO Enterprise Events

Date	Event
July 13, 2026	Technical Talk with RF
July 23, 2026	Future of Path Ratings in the Western Interconnection
July 29, 2026	SERC IBR Seminar #3

Slido.com

slido

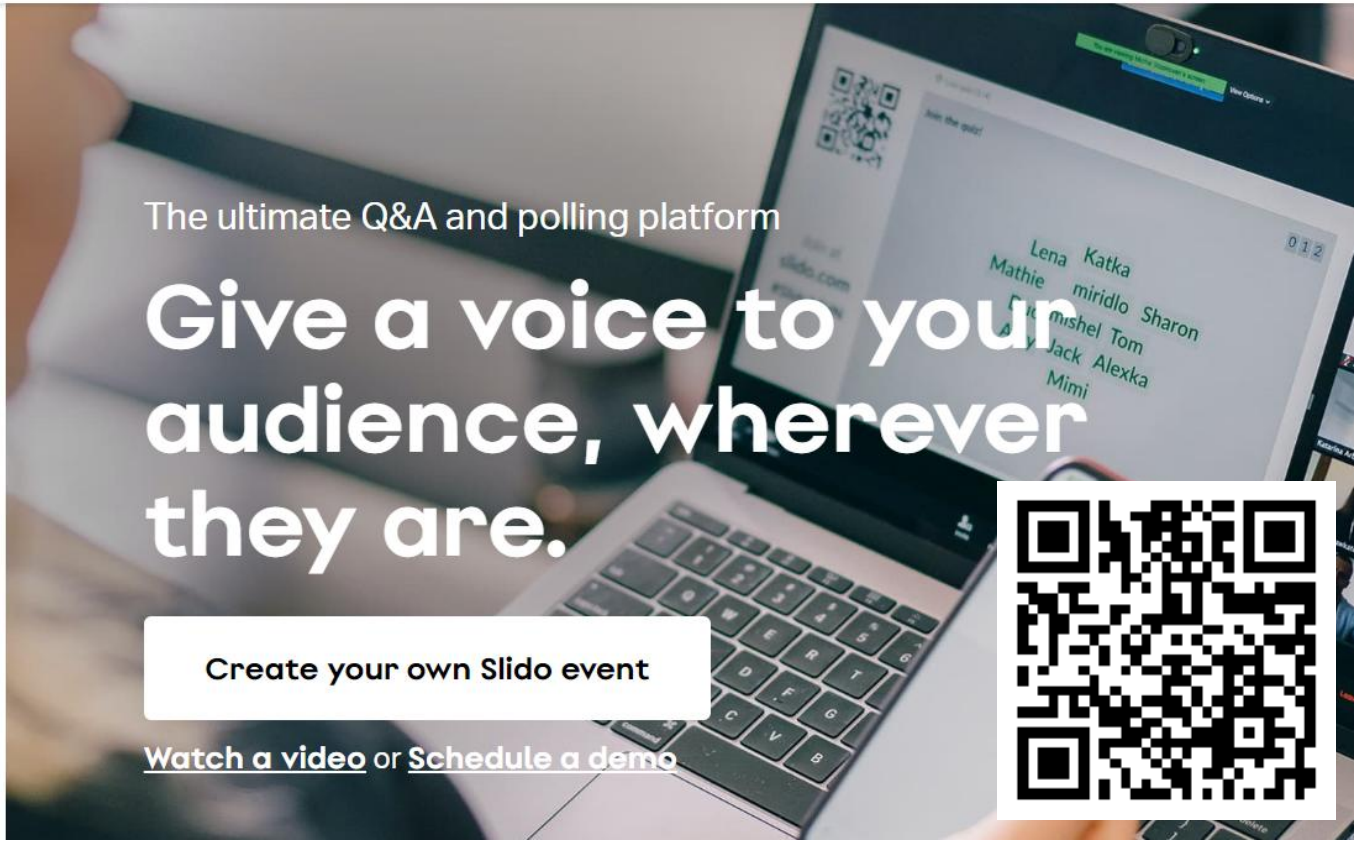
Product Solutions Pricing Resources Enterprise Log In **Sign Up**

#TXRE

Joining as a participant?

Enter event code

Join an existing event



Agenda

- The Supply Chain
- Key Definitions
- Related Standards
- Timeline
- Additional Resources

The Supply Chain

What is the Supply Chain?

Why is this a Security Concern?

Definitions

Vendor *Not a NERC Defined Term

BES Cyber Systems (BCS)

Electronic Access Control or Monitoring System (EACMS)

Physical Access Control System (PACS)

Protected Cyber Asset (PCA)

Related Standards

CIP-013-2 R1 Part 1.1

One or more processes used in planning for the procurement of BCS and their associated EACMS and PACS to identify and assess cyber security risks to the BES from vendor products or services resulting from:

- (i) procuring and installing vendor equipment and software
- (ii) transitions from one vendor to another vendor

Related Standards

CIP-013-2 R1 Part 1.2

One or more processes used in procuring BCS, and their associated EACMS and PACS, that address the following, as applicable:

1.2.1 Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2 Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3 Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4 Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5 Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BCS and their associated EACMS and PACS;

1.2.6 Coordination of controls for vendor-initiated remote access.

Related Standards

CIP-010-4 R1

Part 1.1

Develop a baseline configuration, individually or by group, which shall include the following items:

1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;

1.1.2. Any commercially available or open-source application software (including version) intentionally installed;

1.1.3. Any custom software installed;

1.1.4. Any logical network accessible ports; and

1.1.5. Any security patches applied.

Part 1.6

Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source:

1.6.1. Verify the identity of the software source;

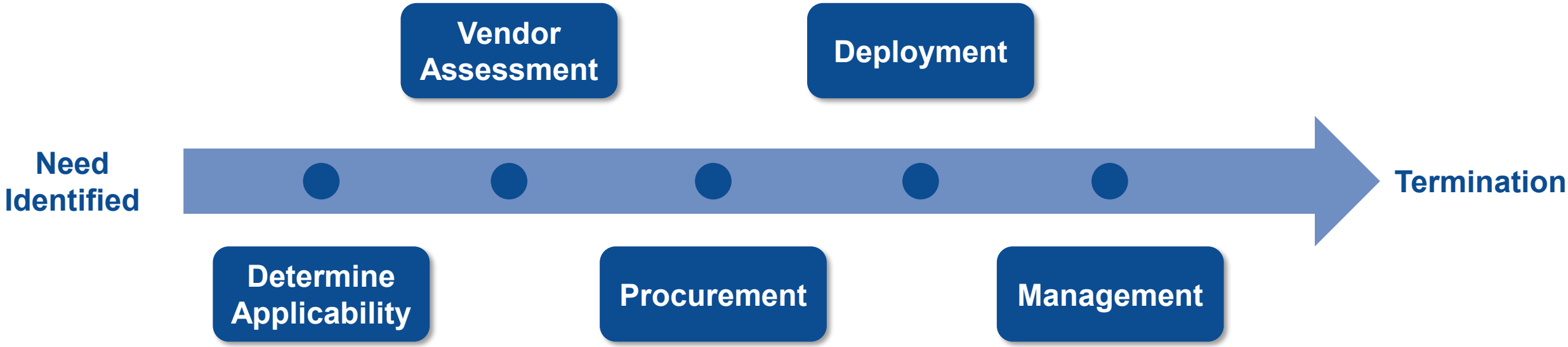
1.6.2. Verify the integrity of the software obtained from the software source.

Related Standards

CIP-007-6 R2 Part 2.3

- For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions:
  - Apply the applicable patches
  - Create a dated mitigation plan
  - Revise an existing mitigation plan
- Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.

Supply Chain Timeline



Additional Resources

CISA

E-ISAC

CIPWG

NATF CIP-013 Implementation Guidance

Technical Rational Documents

Questions?

TEXAS RE
Ensuring electric reliability for Texans