TEXAS RE

Cyber Security – Supply Chain Risk Management

CIP-013-2 R1 & R2

Kerrick Rosemond Jr.
CIP Cyber and Physical Security Analyst

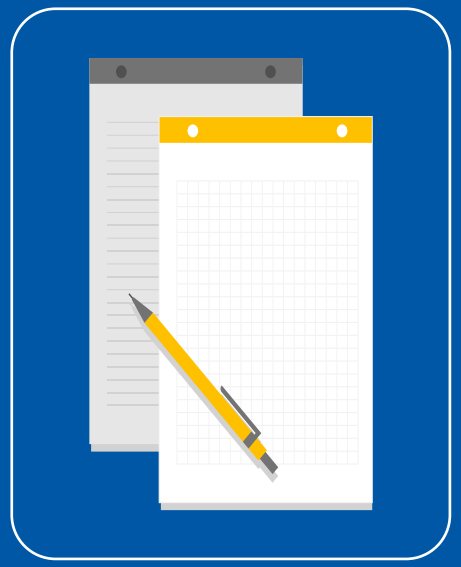
October 3, 2025

CMEP IP Risk Element Areas of Focus: Supply Chain

CIP-013-2 R1, R2 Cyber Security-Supply Chain Risk Management

Rationale	Standard	REQ	Entities for Attention
Mitigate risks to the reliable operation of the BES by implementing sound Supply Chain policies and procedures.	CIP-013-2	CIP-013-2	• Balancing Authority • Distribution Provider • Generator Operator • Generator Owner • Reliability Coordinator • Transmission Operator • Transmission Owner

CIP-013-2 Requirement 1



Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS)

CIP-013-2 Part 1.1 and Part 1.2

1.1 One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from:

- Procuring and installing vendor equipment and software; and
- Transitions from one vendor(s) to another vendor(s)

1.2: One or more process(es) used in procuring BES Cyber Systems, 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
1.2.2. Coordination of responses to vendor-identified incidents related to the products or services
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
1.2.6. Coordination of controls for vendor-initiated remote access.

CIP-013-2 Requirement 2

Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1

Internal Controls

- Supplier Risk Assessment
- Security Requirements for Suppliers
- Monitoring Supplier Compliance
- Access Controls
- Incident Response Plan

TEXAS RE
Ensuring electric reliability for Texans