TEXAS RE

CIP-010-4 R1

Devin Ferris
Manager, CIP Compliance Monitoring

September 5, 2025

Risk Element Areas of Focus: Supply Chain

CIP-010-4 R1: Configuration Change Management

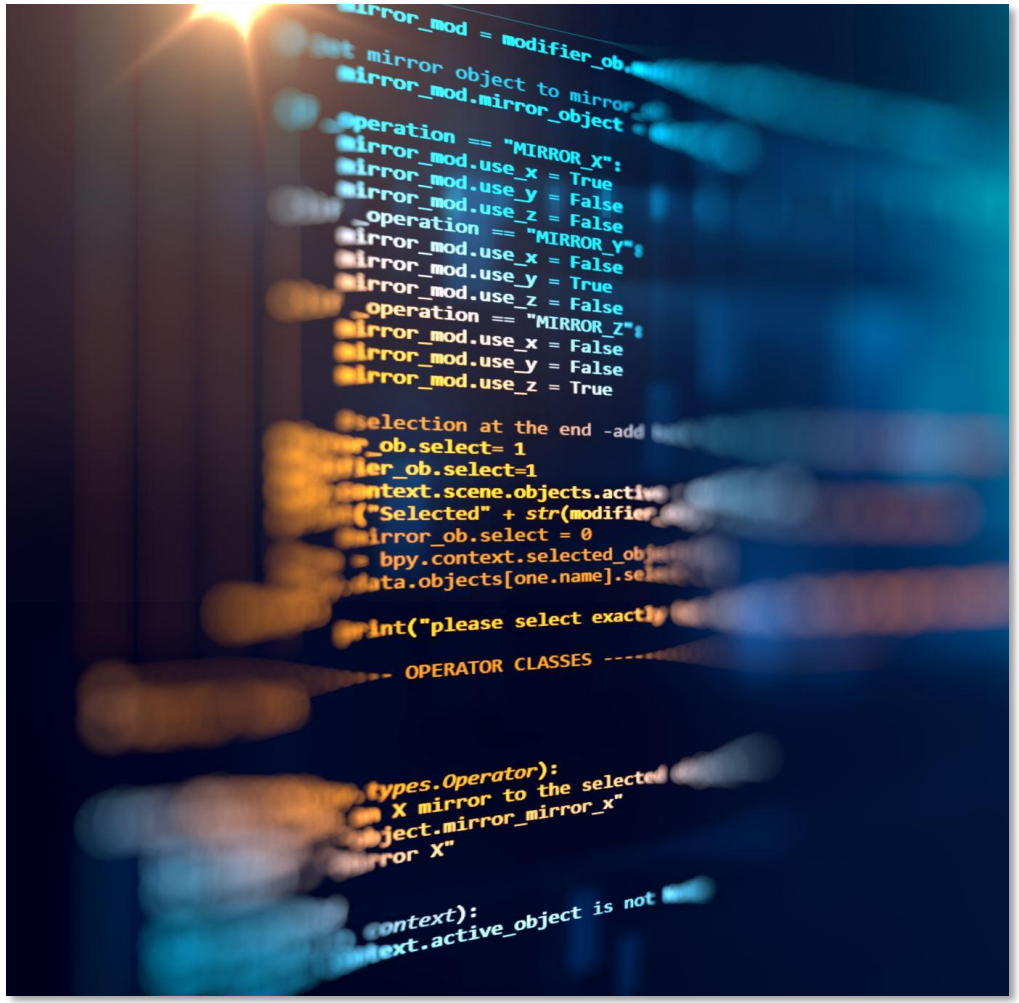
Table 3: Supply Chain

Rationale	Standard	Req	Entities for Attention
Unverified software sources and the integrity of their software may introduce malware or counterfeit software.	CIP-010-4	R1	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner

CIP-010-4 R1, Part 1.6 Abridged Language

For baseline changes related to Parts 1.1.1, 1.1.2, and 1.1.5, with a method available to do so:

- Verify the identity of the software source; and
- Verify the integrity of the software obtained from the software source.



NIST Control Example

CM-14 SIGNED COMPONENTS

Control: Prevent the installation of [*Assignment: organization-defined software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

Discussion: Software and firmware components prevented from installation unless signed with recognized and approved certificates include software and firmware version updates, patches, service packs, device drivers, and basic input/output system updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures is a method of code authentication.

Related Controls: CM-7, SC-12, SC-13, SI-7.

References: [IR 8062].

Asset Inventory Guidance for Owners and Operators

https://www.cisa.gov/resources-tools/resources/foundations-ot-cybersecurity-asset-inventory-guidance-owners-and-operators

TEXAS RE
Ensuring electric reliability for Texans