TEXAS RE

2026 CMEP IP Risk Element – Grid Transformation CIP-004-7 R6

Rebekah Barber
CIP Compliance Team Lead

June 5, 2026

Risk Focus & CMEP IP Risk Factors

Risk Elements
Remote Connectivity
Supply Chain
Physical Security
Grid Transformation
Facility Ratings
Extreme Weather Response

Key Definition – BCSI

BES Cyber System Information (BCSI)

Sensitive data that could allow unauthorized access to the Bulk Electric System, specific to actionable information that poses a direct security threat. It excludes out of context and isolated technical details like individual IP addresses or device names.

CIP-004-7 R6 – Access Management for BCSI

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" that collectively include each of the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information*.

To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys).

CIP-004-7 R6 – Access Management for BCSI

Part 6.1: Access Authorization

- Entities must authorize provisioned access to Bulk Electric System Cyber System Information (BCSI) prior to granting it, ensuring it is based on business need as determined by the entity.

Part 6.2: Access Verification

- Entities must verify at least once every 15 calendar months that all active provisioned access to BCSI remains authorized and aligned with the individuals ongoing job requirements.

Part 6.3: Access Revocation

- Entities must remove an individual's provisioned access to BCSI by the end of the next calendar day following a termination action.

Best Practices and Additional Resources

Best Practices

- Centralized access administration
- Enforce least privilege
- Audit access logs

Resources

- Implementation Guidance
- Technical Rational
- NIST SP 800-53 Rev. 5.

Questions?

TEXAS RE
Ensuring electric reliability for Texans