BCSI in the Cloud

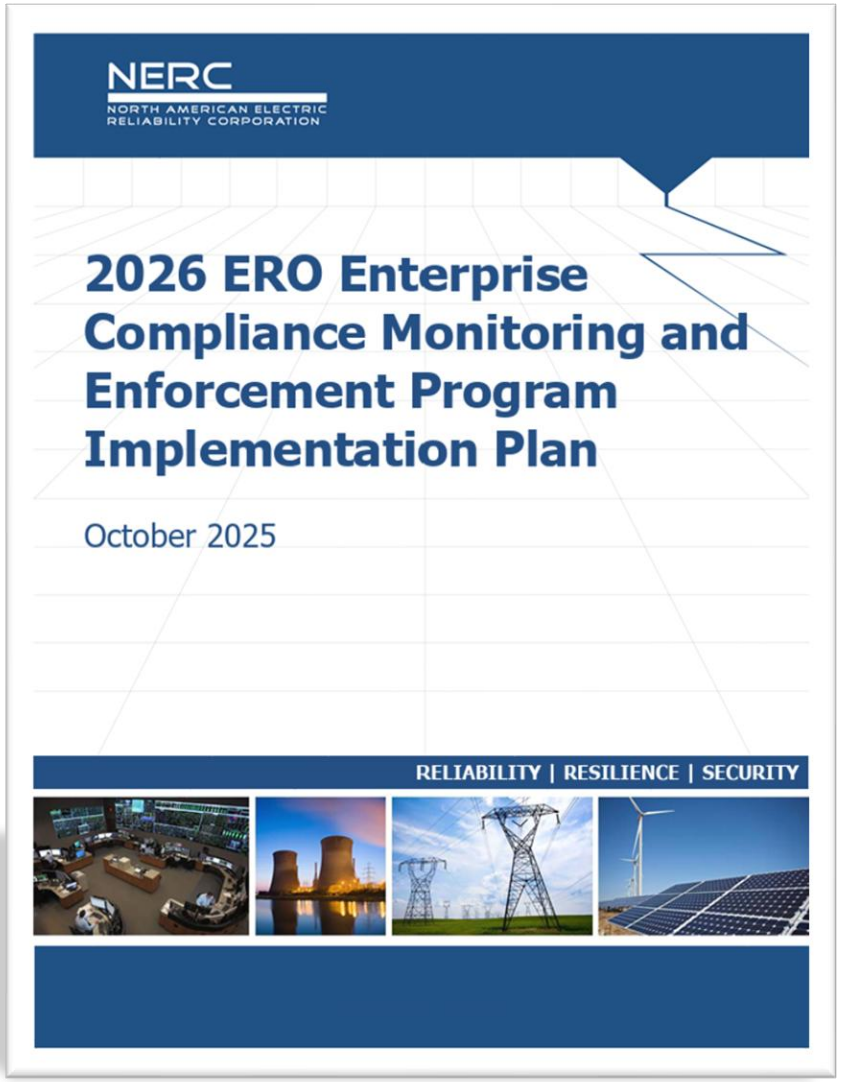
Gabriela Barragan
CIP Cyber & Physical Security Analyst

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.

2026 CMEP IP



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

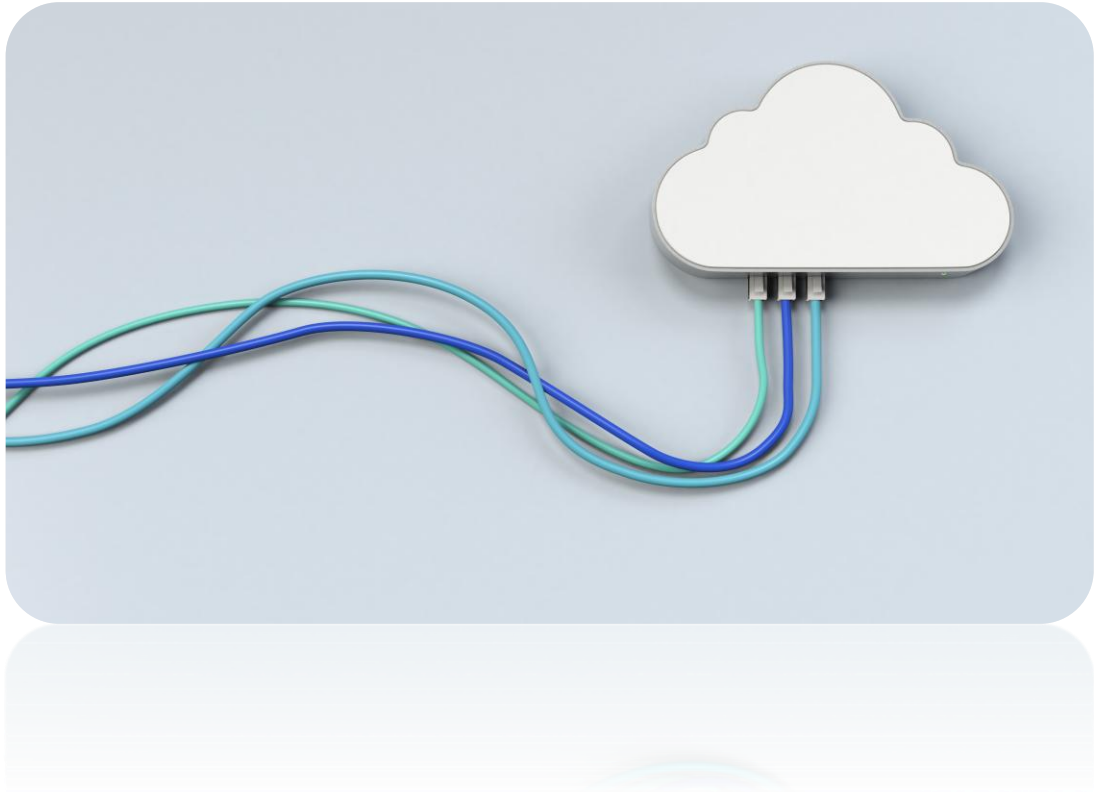
Risk Element: Grid Transformation

CIP-004-7 R6

- Address access control for BES Cyber System information.

CIP-011-3 R1

- Address information protection.



CIP-004: Personnel & Training

CIP-004-6

- Designated Storage Location
- Access Management

CIP-004-7

- Provisioned Access
- New Requirement R6

CIP-011: Information Protection

CIP-011-2

- Location Dependent: Designated Storage Locations

CIP-011-3

- Objective Focused

Risks of BCSI in the Cloud

Technical and Security Risks

- Shared infrastructure vulnerabilities/supply chain
- Encryption key management
- Data sovereignty

Operational Risks

- Reduced visibility
- Cloud service outages

What is BCSI?

BCSI is information about Bulk Electric System (BES) Cyber Systems that:

- Is not publicly available
- Could facilitate unauthorized access or misuse
- Could impact reliable operation of the BES

CIP-011-3 R1 Part 1.1 and Part 1.2

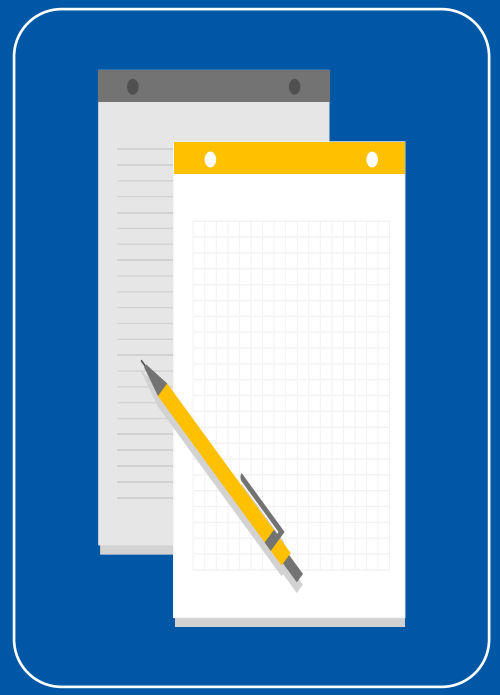
Part 1.1

- Method(s) to identify BCSI

Part 1.2

- Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality

CIP-004-7 R6: What is Access?



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

BCSI Access Management Lifecycle

Part 6.1

Prior to provisioning, authorize (unless already authorized according to Part 4.1) based on the need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

6.1.1. Provisioned electronic access to electronic BCSI; and

6.1.2. Provisioned physical access to physical BCSI

Part 6.2

Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI:

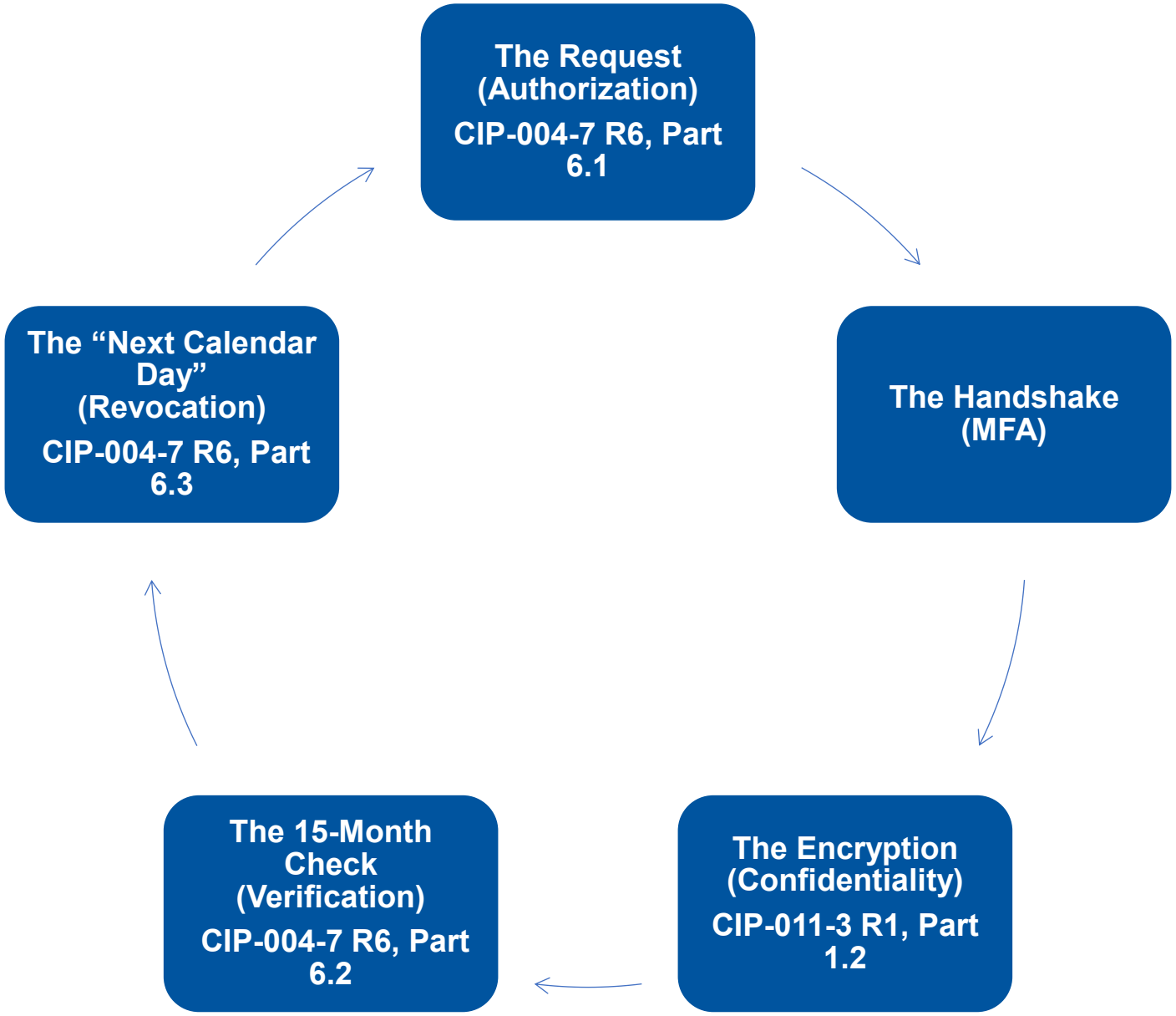
6.2.1 have an authorization record; and

6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity

Part 6.3

For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action

Example: BCSI Access Request and Revocation



The Shared Responsibility Model

Cloud Service Provider

The Entity

The Compliance Line

CIP-004-7 Best Practices & Internal Controls

Best Practices

- ❑ Role-Based Access Control
- ❑ Just-In-Time Access

Internal Controls

- ❑ Access Provisioning Logs
- ❑ Verification Reports

CIP-011-3 Best Practices & Internal Controls

Best Practices

- ❑ Separation of Duties for Key Management
- ❑ Disposal Verification Logging

Internal Controls

- ❑ Key Management Policy
- ❑ Cryptographic Controls

Resources

- NERC Implementation Guidance: Cloud Solutions for BCSI
- NERC Security Guideline: Primer for Cloud and BCSI Protection
- NERC Security Guideline: BCSI Cloud Encryption
- NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing

Contact

Compliance@TexasRE.org