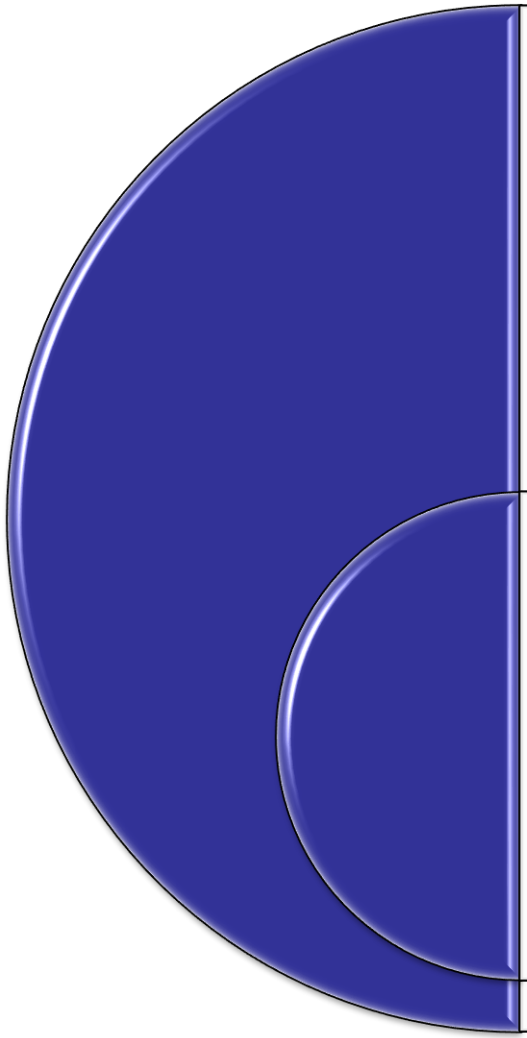
TEXAS RE

BCSI in the Cloud CIP-004-7 and CIP-011-3

Devin Kitchens
Manager, CIP Compliance Monitoring

BES Cyber System Information (BCSI)



Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements.

Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System

CIP-011-3: Cyber Security – Information Protection

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.

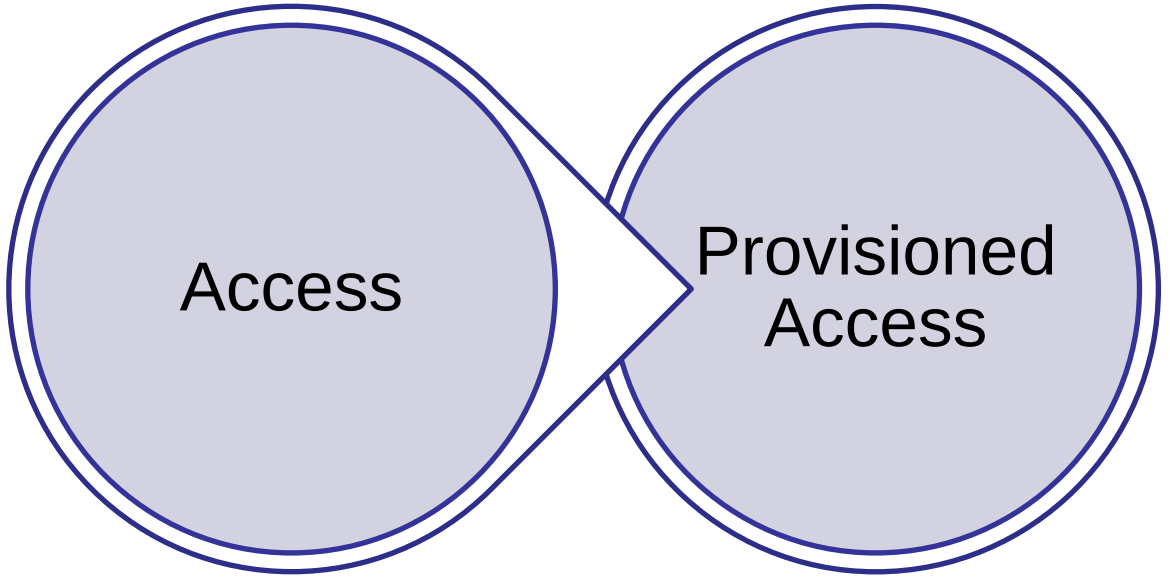
CIP Evidence Request Tool

- **CIP Evidence Request Tool Level 1 Requests**
  - Documented process, plan, procedure, program etc.
- **CIP Evidence Request Tool Level 2 Requests**
  - Implementation evidence

CIP-004-7: Cyber Security – Personnel & Training

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on 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.	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

Key Words



Resources

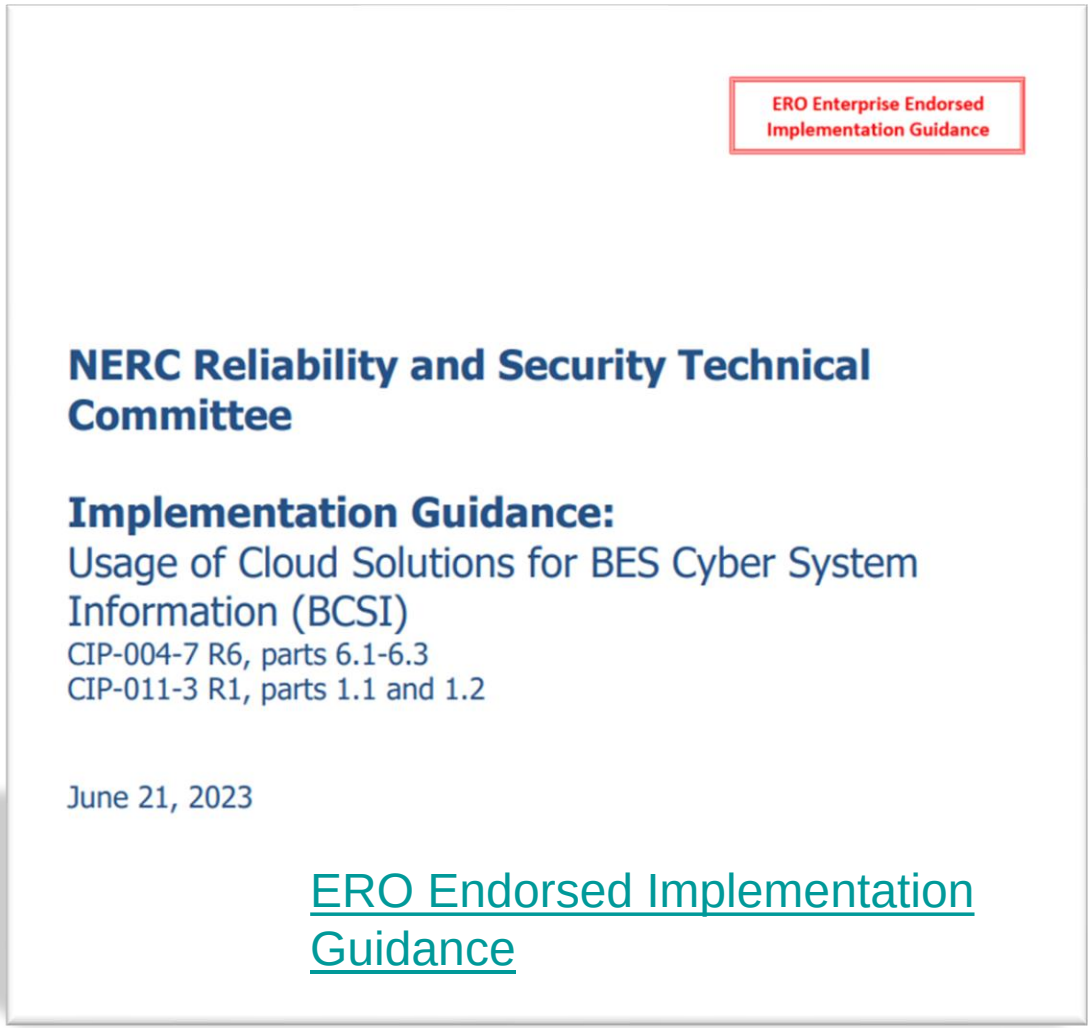
- Technical Rational
- NERC Glossary of Terms
- Engagement Common Questions – NIST Controls
- ERO Enterprise Endorsed Implementation Guidance

Resources Continued

Standard	Req.	Part	Question	Mapping of CIP Standards to NIST Cybersecurity Framework (CSF) v1.1
CIP-011-3	R1		Provide evidence and explain in detail, if [EntityAcr] generates diagrams for CIP-005 that include data flows for logical and physical connectivity?	ID.AM-3
CIP-011-3	R1		Provide evidence and explain in detail, if [EntityAcr]'s data flow diagrams are classified according to the sensitivity of the information?	ID.AM-3
CIP-011-3	R1		Provide evidence and explain in detail, if [EntityAcr] has implemented processes or procedures to identify and secure protected information at rest and data in transit?	PR.DS-1, PR.DS-2
CIP-011-3	R1, R2		Provide evidence and explain in detail, if [EntityAcr] has a process for an information protection program, and does it consist of policy controls such as document markings, secure handling procedures, or secure destruction procedures?	PR.DS-5
CIP-011-3	R1, R2		Provide evidence and explain in detail, if [EntityAcr]'s information protection program has technical controls in place, such as access control, encryption, or digital loss prevention?	PR.DS-5
CIP-011-3	R2		Provide evidence and explain in detail, if [EntityAcr] implements procedures to sanitize media containing protected information prior to disposal, release out of organization control, or release for reuse?	PR.DS-1, PR.DS-3
CIP-011-3	R2		Provide evidence and explain in detail, if [EntityAcr] has mechanisms that sanitize information to the strength and integrity commensurate with the security category or classification of the information?	PR.DS-1, PR.DS-3
CIP-011-3	R2		Provide evidence and explain in detail, if [EntityAcr] implements a management control process that evaluate a sampling of retired systems to ensure data is no longer accessible?	PR.IP-6

Engagement Common Questions

Resources Continued


ERO Enterprise Endorsed Implementation Guidance

NERC Reliability and Security Technical Committee

Implementation Guidance:
Usage of Cloud Solutions for BES Cyber System Information (BCSI)
CIP-004-7 R6, parts 6.1-6.3
CIP-011-3 R1, parts 1.1 and 1.2

June 21, 2023

[ERO Endorsed Implementation Guidance]

TEXAS RE
Ensuring electric reliability for Texans