NERC

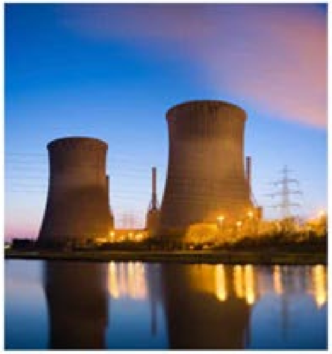
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

BCSI Access Management

Project 2019-02

BCSI SDT
April 27, 2021

RELIABILITY | RESILIENCE | SECURITY



Administrative Items

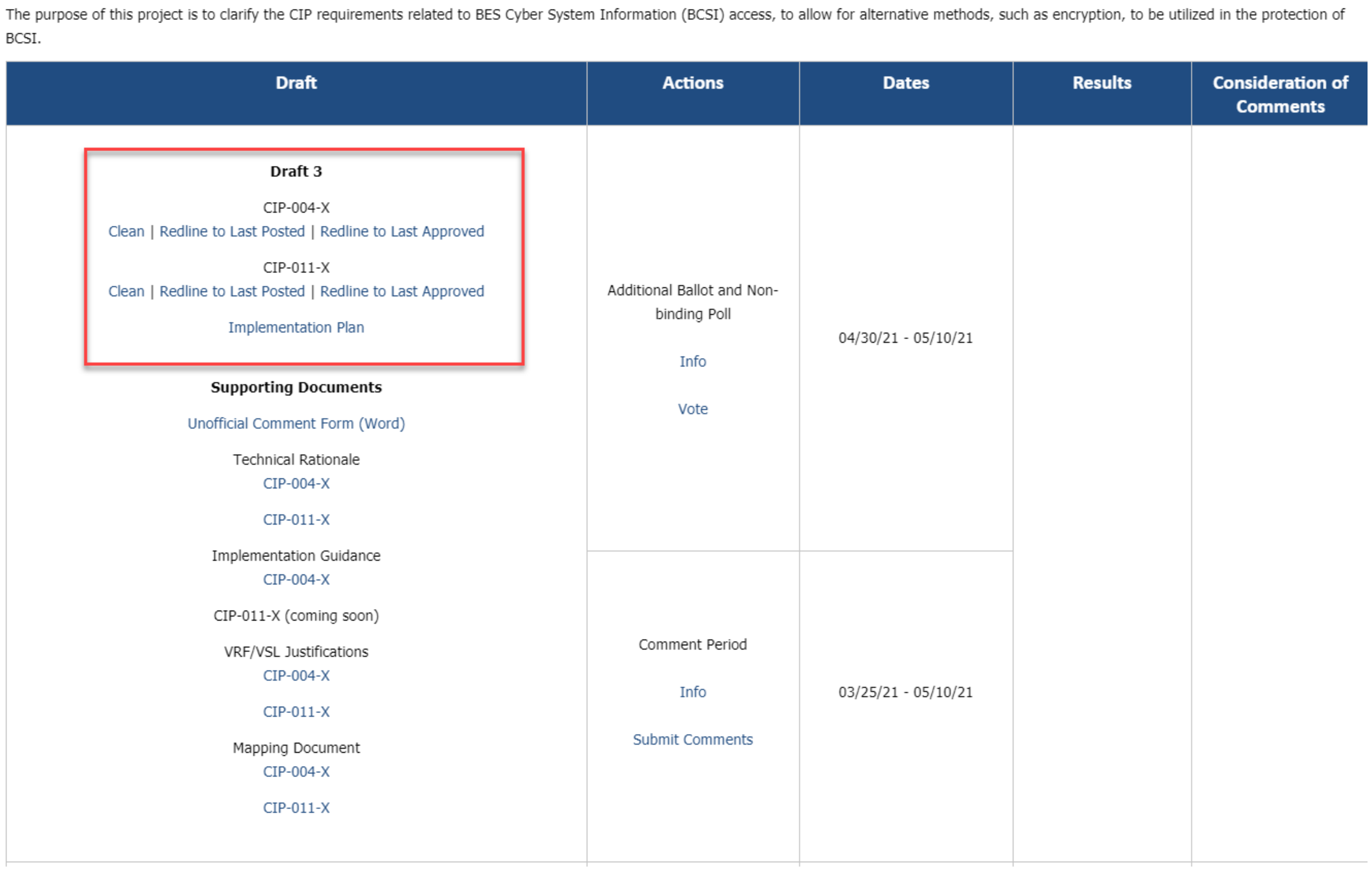
- NERC Antitrust Guidelines
  - It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.
- Notice of Open Meeting
  - Participants are reminded that this webinar is public. The access number was widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Agenda

Draft 3 – BES Cyber System Information (BCSI)

- 2019-02 Standards Authorization Request (SAR)
- Modifications to:
  - CIP-004-X
  - CIP-011-X
  - Implementation Plan
- Next Steps
- Q&A

2019-02 - Draft 3 Materials



The purpose of this project is to clarify the CIP requirements related to BES Cyber System Information (BCSI) access, to allow for alternative methods, such as encryption, to be utilized in the protection of BCSI.

Draft	Actions	Dates	Results	Consideration of Comments
Draft 3 CIP-004-X Clean | Redline to Last Posted | Redline to Last Approved CIP-011-X Clean | Redline to Last Posted | Redline to Last Approved Implementation Plan **Supporting Documents** Unofficial Comment Form (Word) Technical Rationale CIP-004-X CIP-011-X Implementation Guidance CIP-004-X CIP-011-X (coming soon) VRF/VSL Justifications CIP-004-X CIP-011-X Mapping Document CIP-004-X CIP-011-X	Additional Ballot and Non-binding Poll Info Vote	04/30/21 - 05/10/21		
	Comment Period Info Submit Comments	03/25/21 - 05/10/21		

2019-02 SAR

- BES Cyber System Information Access Management SAR
  - Approved in August 2019
- Purpose/Goal
  - Enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage BCSI
  - Provide a secure path toward the use of modern third-party data storage and analysis solutions (aka cloud services)
  - Enable the CIP Standards to allows for alternative methods, such as encryption, to be utilized in the protection of BCSI
  - Clarify CIP-004 and CIP-011 requirements related to both managing access and protecting BCSI
  - Allow for methods other than storage location to be used, such as encryption, while still permitting Registered Entities to define how BCSI is protected.

Distinction in Purpose

- CIP-004
  - Manage individuals’ access to BCSI
  - Where access can be provisioned

- CIP-011
  - Protect BCSI from unauthorized access
  - Wherever it is located

How we meet the SAR

CIP-004-X

1. BCSI access mgmt consolidated into one requirement
2. “Storage locations” is no longer explicitly stated
3. Changed to “provisioned access to BCSI”
4. Included concept of “obtain and use”
5. Clarified requirements for physical and electronic

CIP-011-X

1. Keeping it simple, yet focused
2. Focus on BCSI that pertains to the Applicable Systems
3. Mitigating the risk of compromising BCSI confidentiality

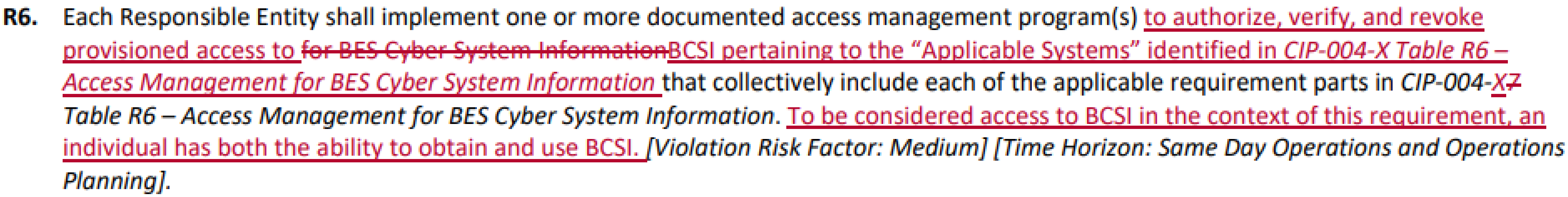
Backwards Compatibility for Storage Locations

- Addresses hindrance to using cloud
- Less prescriptive language enables other methods (e.g., encryption) for access management
- Entities can still use designated storage locations

Provisioned Access

- “provisioned access” is a noun
- Scopes what kind of access CIP-004 R6 requirements pertain to
  - Specific mechanisms available and feasible to provision access
  - NOT what someone views or hears
  - Intended to provide means to obtain and use BCSI
- All other “access” is considered in CIP-011 program

CIP-004-X



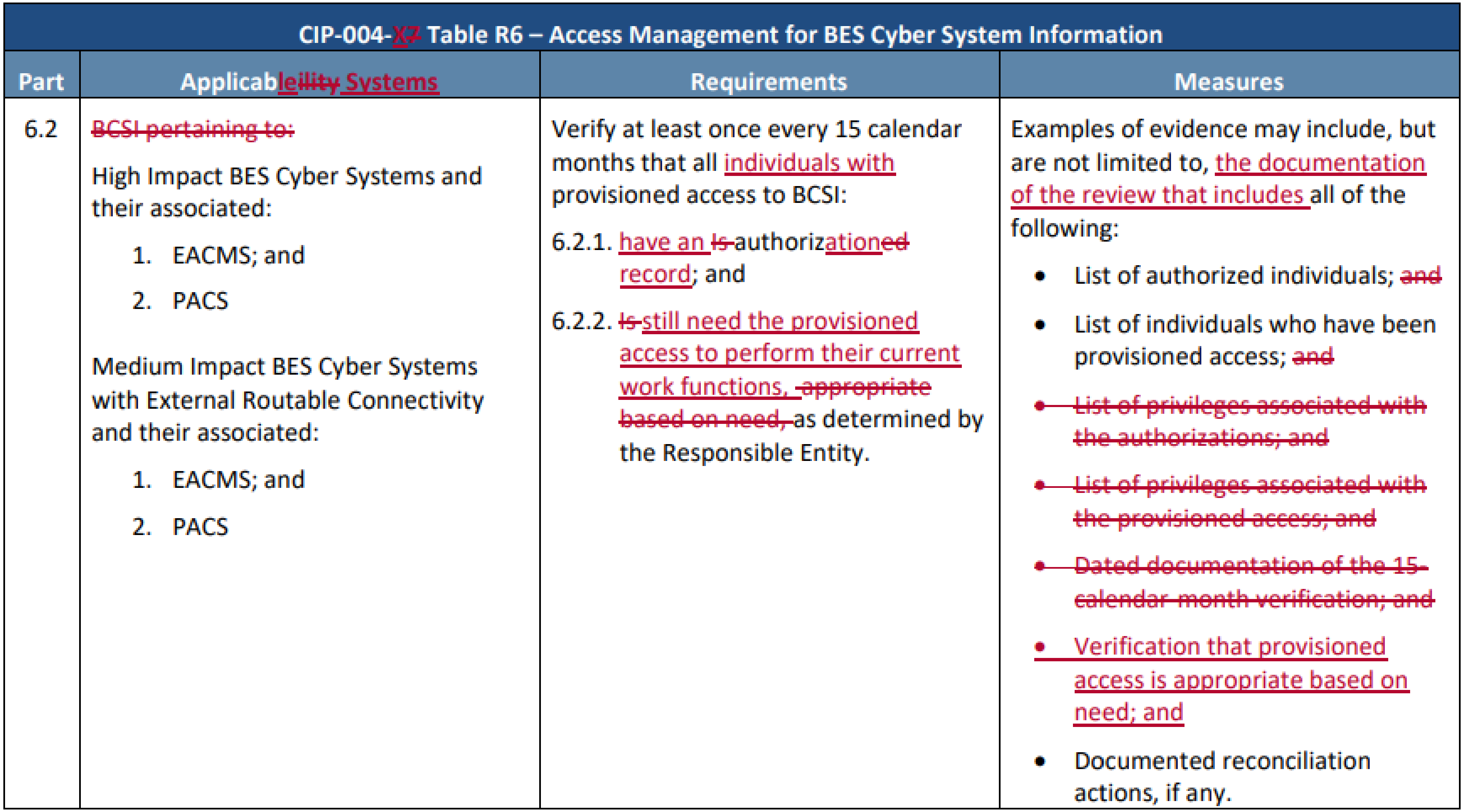
R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to ~~for BES Cyber System Information~~BCSI pertaining to the “Applicable Systems” identified in *CIP-004-X Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-X~~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. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]*.

- authorize, verify, and revoke provisioned access
- applicable systems
- obtain and use

CIP-004-X

CIP-004-X~~7~~ Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable~~ility~~ Systems**	**Requirements**	**Measures**
6.1	~~BCSI pertaining to:~~ 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, ~~A~~authorize (unless already authorized according to Part 4.1.)~~provisioning of access to BCSI~~ based on need~~ (unless already authorized according to Part 4.1.)~~, 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. Note: 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).	Examples of evidence may include, but are not limited to, ~~the following:~~ individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access. • ~~Dated authorization records for provisioned access to BCSI based on need; or~~ • ~~List of authorized individuals~~

CIP-004-X

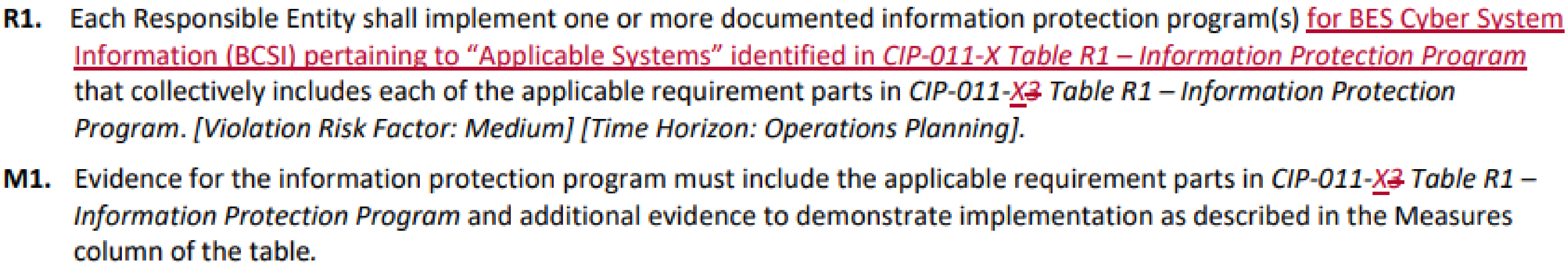


CIP-004-X~~7~~ Table R6 – Access Management for BES Cyber System Information			
Part	Applicable~~ility~~ Systems	Requirements	Measures
6.2	~~BCSI pertaining to:~~ High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an ~~Is~~ authorization~~ed~~ record; and 6.2.2. ~~Is~~ still need the provisioned access to perform their current work functions, ~~appropriate based on need,~~ as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; ~~and~~ • List of individuals who have been provisioned access; ~~and~~ ~~• List of privileges associated with the authorizations; and~~ ~~• List of privileges associated with the provisioned access; and~~ ~~• Dated documentation of the 15-calendar month verification; and~~ • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.

CIP-011-X

- CIP-011-3 R1 Parts 1.3 and 1.4 were deleted.

CIP-011-X

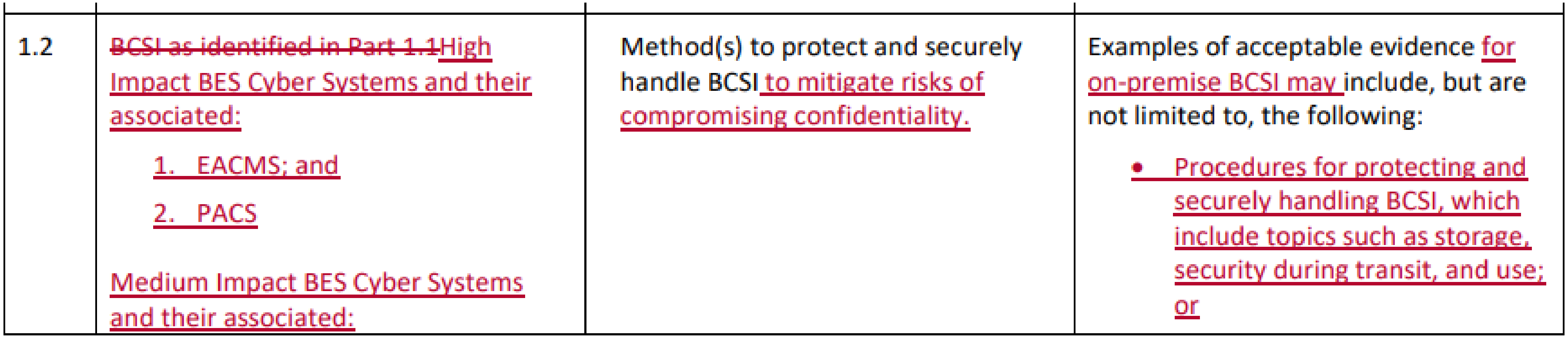


R1. Each Responsible Entity shall implement one or more documented information protection program(s) for BES Cyber System Information (BCSI) pertaining to "Applicable Systems" identified in *CIP-011-X Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-X~~3~~ Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-X~~3~~ Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

- Removed "BCSI pertaining to" from the Applicable System column and added language to R1 parent requirement.

CIP-011-X Requirement R1 Part 1.2.



1.2	~~BCSI as identified in Part 1.1~~High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated:	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of acceptable evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling BCSI, which include topics such as storage, security during transit, and use; or

CIP-011-X
Requirement R1 Part 1.2 Cont.

	1. EACMS; and 2. PACS		• Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or • Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

Implementation Plan

- Effective Date
  - 24 months from governmental approval date
  - Compliance dates for early adoption of revised CIP standards

Next Steps

- Final Ballot
  - June 2021
- NERC Board of Trustees Adoption
  - November 2021

- Informal Discussion
  - Via the Q&A feature
  - Chat only goes to the host, not panelists
  - Respond to stakeholder questions
- Other
  - Some questions may require future team consideration
  - Please reference slide number, standard section, etc., if applicable
  - Team will address as many questions as possible
  - Webinar and chat comments are not a part of the official project record
  - Questions regarding compliance with existing Reliability Standards should be directed to ERO Enterprise compliance staff, not the Standard Drafting Team.

Questions and Answers