NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2019-02

BES Cyber System Information (BCSI) Access Management

Industry Webinar
August 19, 2020

RELIABILITY | RESILIENCE | SECURITY

Agenda

- Presenters
  - SDT
    - Chair, John Hansen, Exelon
    - Vice Chair, Josh Powers, SPP
    - Member, Conor Martin, Arizona Public Service
    - Member, Regan Plain, Minnkota Power Cooperative
    - Member, William Vesely, Consolidated Edison Company of New York, Inc.
  - NERC Staff
    - Latrice Harkness, Senior Standards Developer
- SDT Team
- Proposed Revisions Overview

Agenda cont'd

- CIP-004 Proposed Changes
- CIP-011 Proposed Changes
- Implementation Plan
- Next Steps
- Questions and Answers

NERC Antitrust

- 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. It is the responsibility of every NERC participant and employee who may in any way affect NERC’s compliance with the antitrust laws to carry out this commitment.

NERC Public Disclaimer

- Public Announcement
  - Participants are reminded that this meeting is public. Notice of the meeting was widely distributed. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.
- Presentation Material
  - Information used herein is used for presentation purposes and may not reflect the actual work of the official posted materials
- For the official record
  - This presentation is not a part of the official project record
  - Comments must be submitted during the formal posting

Standard Drafting Team (SDT)

Name	Organization/ Company
John Hansen (Chair)	Exelon
Josh Powers (Vice Chair)	Southwest Power Pool, Inc. (SPP)
Victoria Bethley	Duke Energy
Sharon Koller	American Transmission Company, LLC
Michael Lewis	Southern California Edison
Conor Martin	Arizona Public Service
Regan Plain	Minnkota Power Cooperative
Joshua Roper	Westar and KCP&L, Evergy Companies
Clay Walker	Cleco Corporate Holdings LLC
William Vesely	Consolidated Edison Company of New York, Inc.

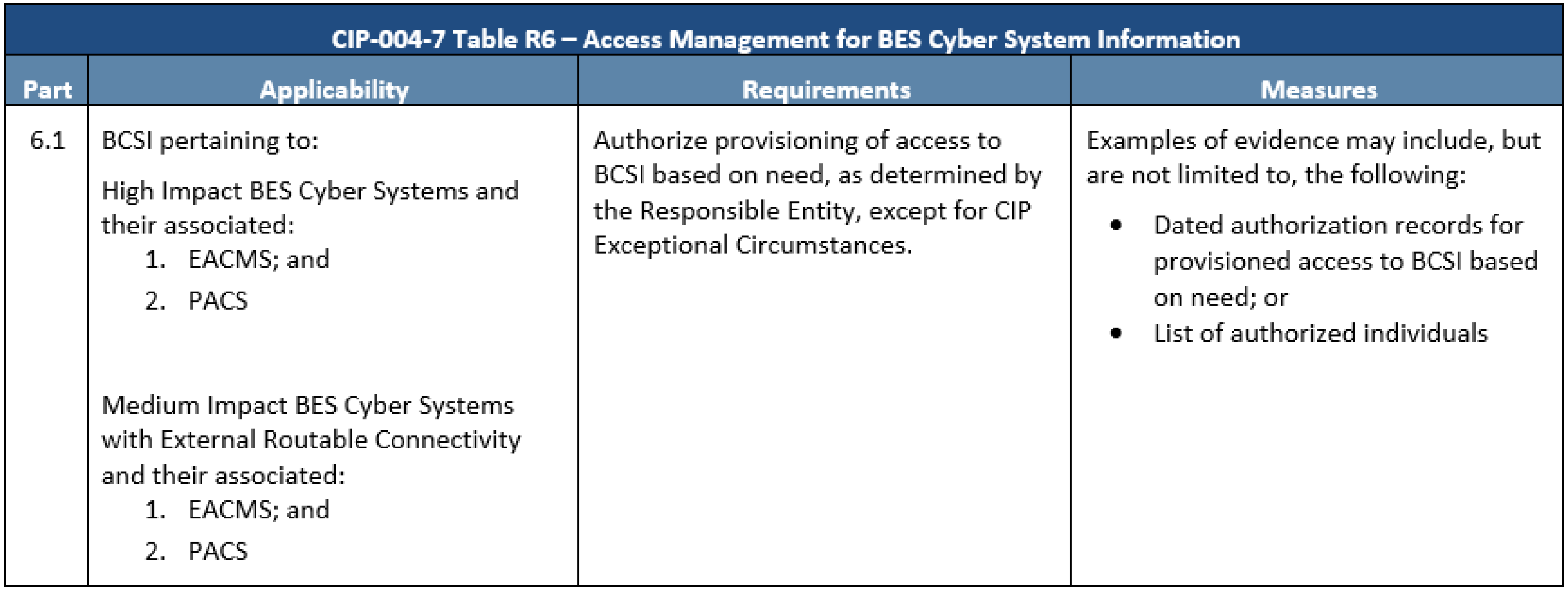
Proposed Revisions Overview

- SDT has met several times since the initial posting to revise standards, complete supporting documentation, and address industry comments
- Overall, SDT was in alignment with industry feedback
- SDT is directionally moving towards:
  - Restoring all BCSI-access-control-related requirements (and “Medium w/ ERC” applicability) in CIP-004-7 under a single requirement (Requirement R6)
  - Clarifying the intent of the BCSI vendor risk assessment as a security and technical control method related to the vendor’s services and not the vendor
  - Broadening the key management requirement to “electronic technical mechanisms to protect BCSI” and moving this new requirement under Requirement R1
  - Clarifying the applicability to, “When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, …”
  - Reverting back to “Method(s)” when changed to “Procedure(s)” or “Process(es)”
  - Removing PCA as applicable
  - Restoring BCA reuse and disposal requirement as approved (now CIP-011-2, R2)

CIP-004-7, Requirement R6

- This requirement supersedes the following:
  - CIP-004-6, Requirement R4, Part 4.1.3
  - CIP-004-6, Requirement R4, Part 4.4
  - CIP-004-6, Requirement R5, Part 5.3
- R6 – Each Responsible Entity shall implement one or more documented access management program(s) for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].
- M6 – Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information and additional evidence to demonstrate implementation as described in the Measures column of the table.

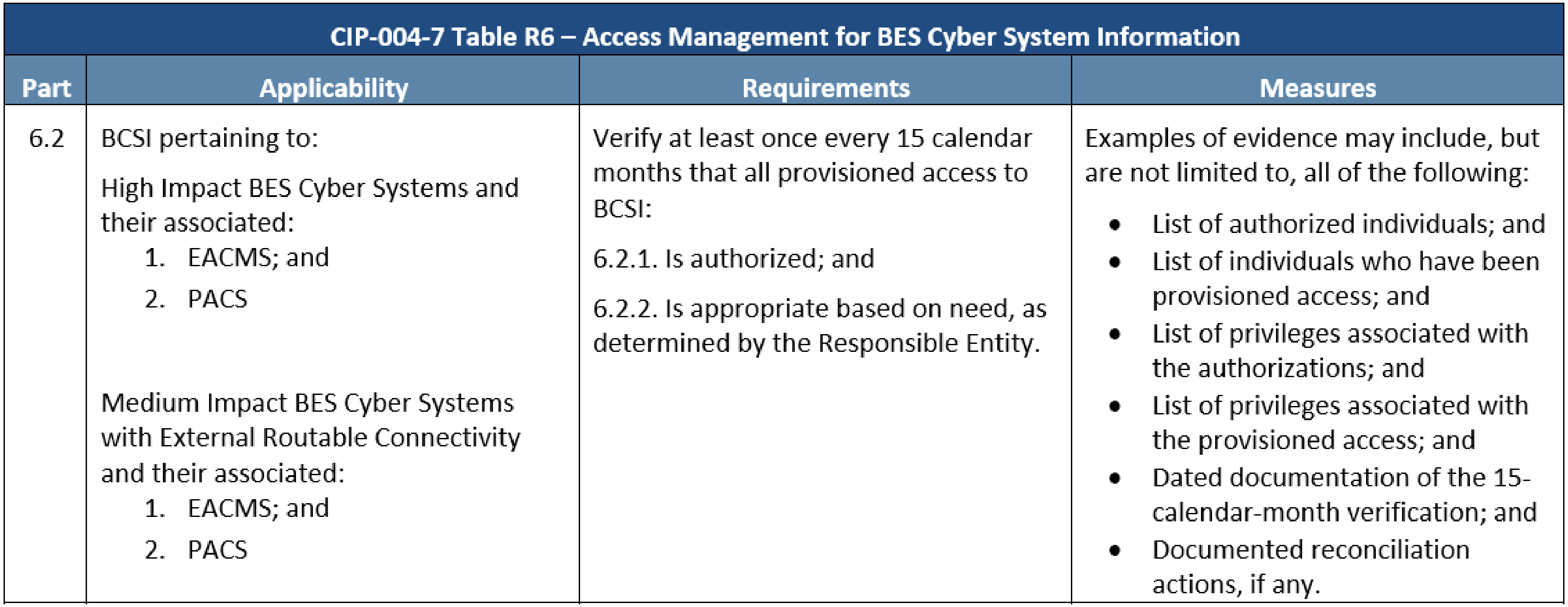
CIP-004-7, Requirement R6, Part 6.1



CIP-004-7 Table R6 – Access Management for BES Cyber System Information

Part	Applicability	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	Authorize provisioning of access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, the following: • Dated authorization records for provisioned access to BCSI based on need; or • List of authorized individuals

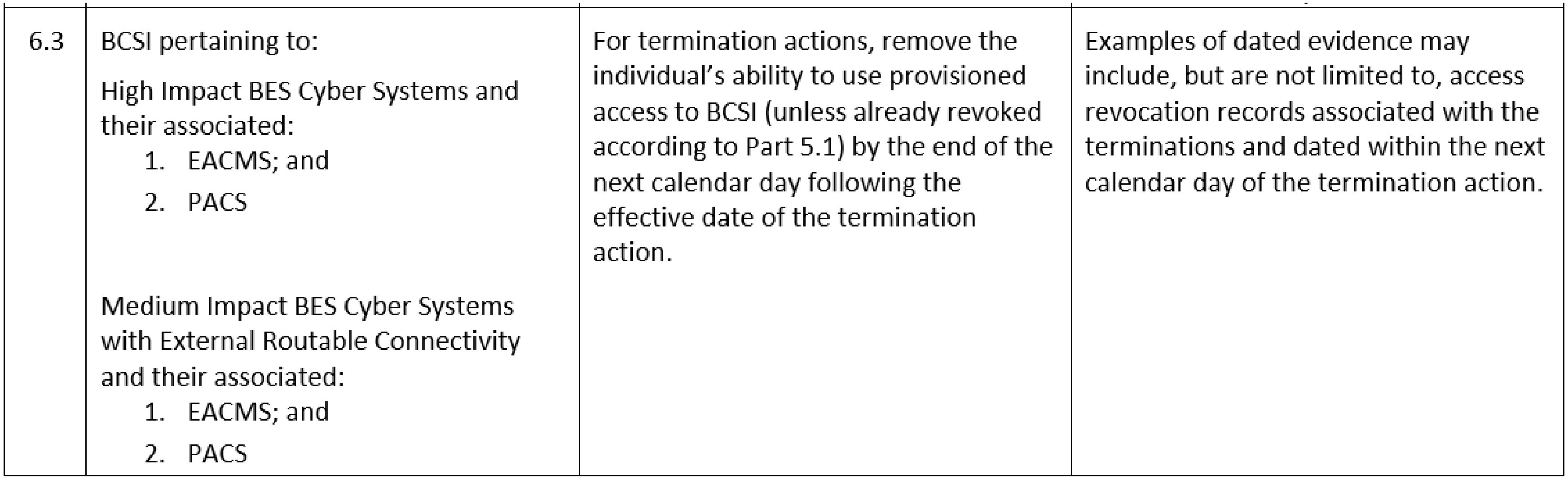
CIP-004-7, Requirement R6, Part 6.2



CIP-004-7 Table R6 – Access Management for BES Cyber System Information

Part	Applicability	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 provisioned access to BCSI: 6.2.1. Is authorized; and 6.2.2. Is appropriate based on need, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, 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 • Documented reconciliation actions, if any.

CIP-004-7, Requirement R6, Part 6.3

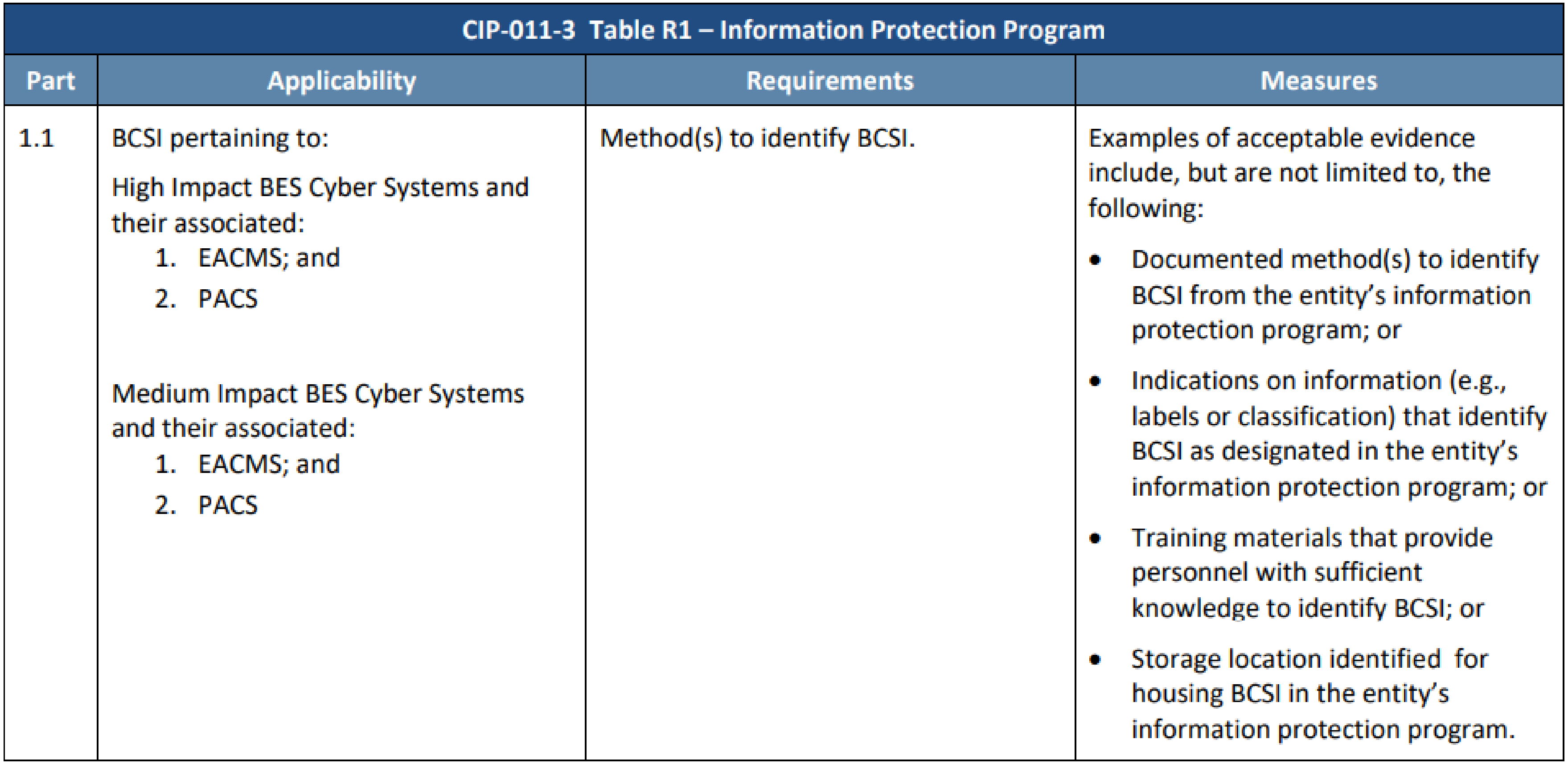


6.3	BCSI pertaining to: High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

CIP-011-3, Requirement R1

- Only changes to parent language = references to new version 3
- R1 – Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 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-011-3 Table R1 – Information Protection Program and additional evidence to demonstrate implementation as described in the Measures column of the table.

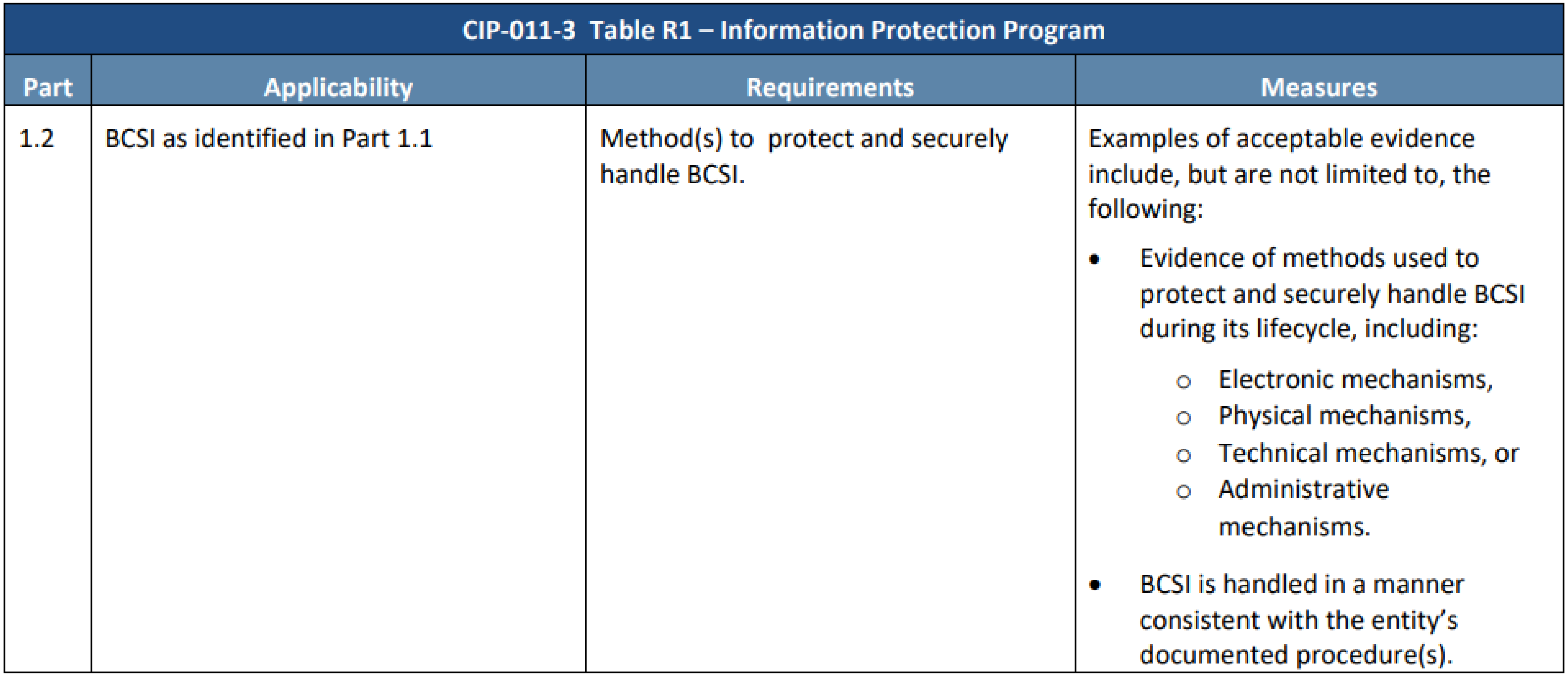
CIP-011-3, Requirement R1, Part 1.1



CIP-011-3 Table R1 – Information Protection Program

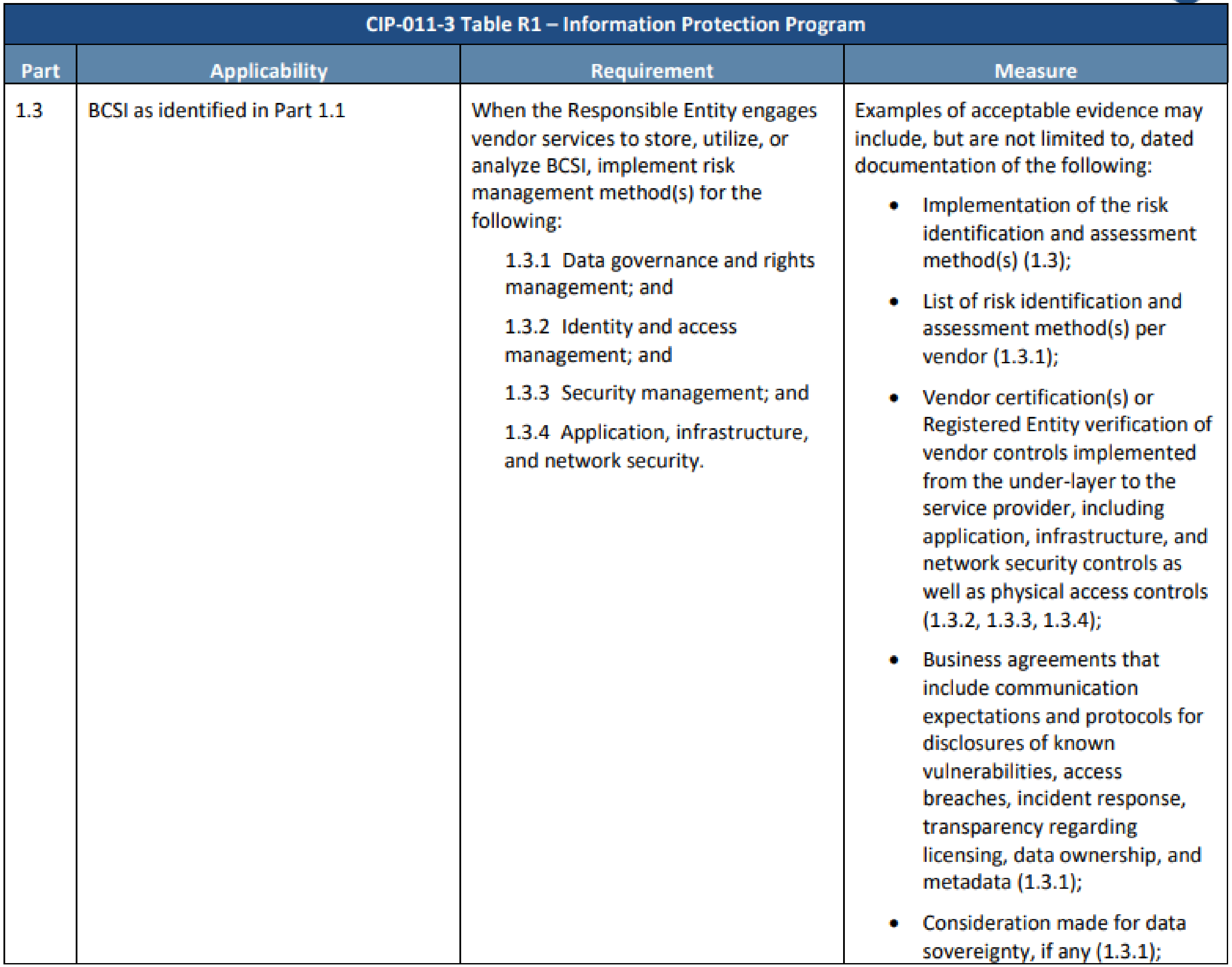
Part	Applicability	Requirements	Measures
1.1	BCSI pertaining to: High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify BCSI.	Examples of acceptable evidence include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage location identified for housing BCSI in the entity's information protection program.

CIP-011-3, Requirement R1, Part 1.2



CIP-011-3 Table R1 – Information Protection Program			
Part	Applicability	Requirements	Measures
1.2	BCSI as identified in Part 1.1	Method(s) to protect and securely handle BCSI.	Examples of acceptable evidence include, but are not limited to, the following: • Evidence of methods used to protect and securely handle BCSI during its lifecycle, including: ○ Electronic mechanisms, ○ Physical mechanisms, ○ Technical mechanisms, or ○ Administrative mechanisms. • BCSI is handled in a manner consistent with the entity's documented procedure(s).

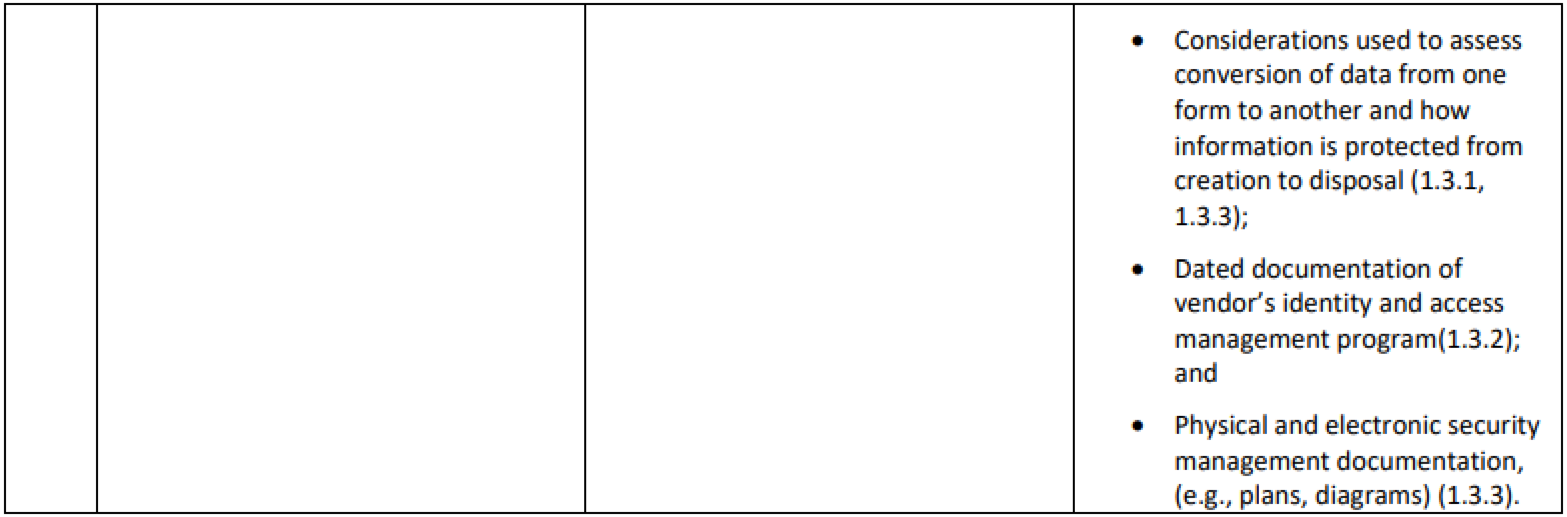
CIP-011-3, Requirement R1, Part 1.3



CIP-011-3 Table R1 – Information Protection Program

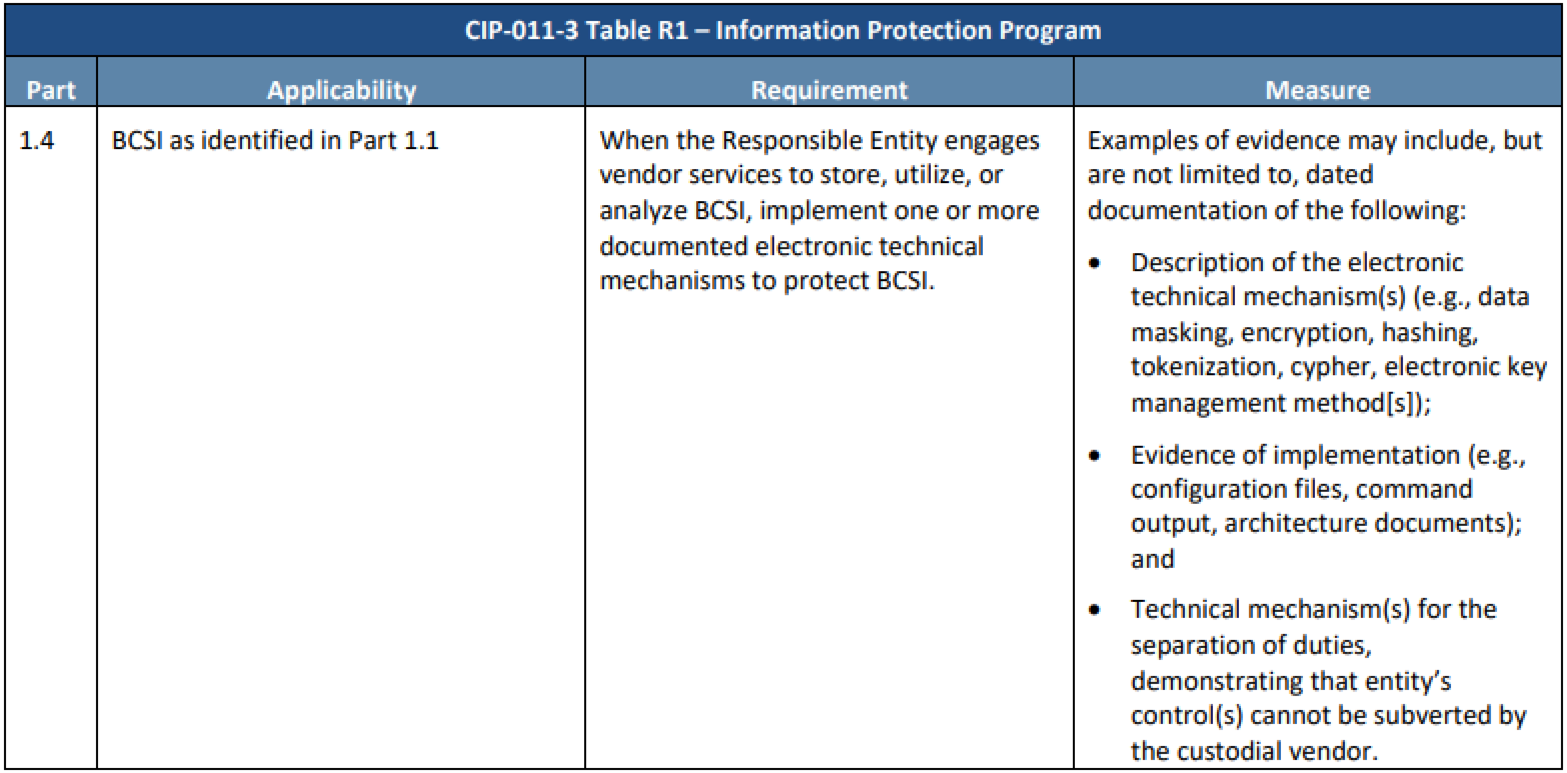
Part	Applicability	Requirement	Measure
1.3	BCSI as identified in Part 1.1	When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement risk management method(s) for the following: 1.3.1 Data governance and rights management; and 1.3.2 Identity and access management; and 1.3.3 Security management; and 1.3.4 Application, infrastructure, and network security.	Examples of acceptable evidence may include, but are not limited to, dated documentation of the following: • Implementation of the risk identification and assessment method(s) (1.3); • List of risk identification and assessment method(s) per vendor (1.3.1); • Vendor certification(s) or Registered Entity verification of vendor controls implemented from the under-layer to the service provider, including application, infrastructure, and network security controls as well as physical access controls (1.3.2, 1.3.3, 1.3.4); • Business agreements that include communication expectations and protocols for disclosures of known vulnerabilities, access breaches, incident response, transparency regarding licensing, data ownership, and metadata (1.3.1); • Consideration made for data sovereignty, if any (1.3.1);

CIP-011-3, Requirement R1, Part 1.3



			• Considerations used to assess conversion of data from one form to another and how information is protected from creation to disposal (1.3.1, 1.3.3); • Dated documentation of vendor's identity and access management program(1.3.2); and • Physical and electronic security management documentation, (e.g., plans, diagrams) (1.3.3).

CIP-011-3, Requirement R1, Part 1.4



CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.4	BCSI as identified in Part 1.1	When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.	Examples of evidence may include, but are not limited to, dated documentation of the following: • Description of the electronic technical mechanism(s) (e.g., data masking, encryption, hashing, tokenization, cypher, electronic key management method[s]); • Evidence of implementation (e.g., configuration files, command output, architecture documents); and • Technical mechanism(s) for the separation of duties, demonstrating that entity's control(s) cannot be subverted by the custodial vendor.

Implementation Plan

- The SDT is proposing an 18-month period, which provides Responsible Entities to:
  - Address the increased scope of the “Applicability” column now present in CIP-004-7, Requirement R6, and CIP-011-3, Requirement R1, which are focused on access to and protection of BCSI
  - Implement electronic technical mechanisms to protect BCSI when Responsible Entities elect to engage vendor services to store, utilize, or analyze BCSI
  - Develop a risk management method(s) when Responsible Entities elect to engage vendor services to store, utilize, or analyze BCSI
  - Establish and/or modify vendor relationships to ensure compliance with the updated CIP-004 and CIP-011

Next Steps

- Next comment period
  - Project 2019-02 page
  - 45 Days: August 6, 2020-September 21, 2020
  - Additional Ballot: September 11-21, 2020
- Point of contact
  - Latrice Harkness, Senior Standards Developer
  - Latrice.Harkness@nerc.net or call 404-446-9728
- Webinar posting
  - 48-72 hours
  - Standards Bulletin

Q & A Objectives

- Q & A
  - Via the Q&A feature
  - 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 and Answers