

## Comment Report

**Project Name:** 2019-02 BES Cyber System Information Access Management (Draft 3)  
**Comment Period Start Date:** 3/25/2021  
**Comment Period End Date:** 5/10/2021  
**Associated Ballots:** 2019-02 BES Cyber System Information Access Management CIP-004-7 AB 3 ST  
2019-02 BES Cyber System Information Access Management CIP-011-3 AB 3 ST  
2019-02 BES Cyber System Information Access Management Implementation Plan AB 3 OT

There were 64 sets of responses, including comments from approximately 157 different people from approximately 98 companies representing 10 of the Industry Segments as shown in the table on the following pages.

## Questions

1. The standards drafting team (SDT) considered industry's concerns about the phrase "provisioning of access" requesting clarity on this terminology. The SDT added "authorize, verify, and revoke provisioned access" to the parent requirement CIP-004-X, Requirement R6, and changed "provisioning of access" to "provisioned access" in the requirement parts. This should clarify the intent that it is a noun which scopes what the Registered Entity must authorize, verify, and revoke, rather than a verb relating to how provisioning should occur. That is up to the entity to determine. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.
2. The SDT considered industry's concerns about the absence of "obtain and use" language from the CMEP Practice Guide, which currently provides alignment on a clear two-pronged test of what constitutes access in the context of utilizing third-party solutions (e.g., cloud services) for BCSI. The SDT mindfully mirrored this language to assure future enforceable standards are not reintroducing a gap. Do you agree this clarifying language makes it clear both parameters of this two-pronged test for "obtain and use" must be met to constitute "access" to BCSI? If not, please provide the basis for your disagreement and an alternate proposal.
3. The SDT considered industry comments regarding the removal of storage locations. The SDT must enable the CIP standards for the use of third-party solutions (e.g., cloud services) for BCSI, and retention of that language hinders meeting those FERC directives. The absence of this former language does not preclude an entity from defining storage locations as the method used within an entity's access management program. CIP-004-X, Requirement R6, is at an objective level to permit more than that one approach. Do you agree the requirement retains the flexibility for storage locations to be used as one way to meet the objective? If not, please provide the basis for your disagreement and an alternate proposal.
4. To address industry comments while also enabling entities to use third-party solutions (e.g., cloud services) for BCSI, in CIP-004-X, Requirement R6 Part 6.1, the SDT made a distinction between "electronic access to electronic BCSI" versus "physical access to physical BCSI". This clarifies physical access alone to hardware containing electronic BCSI, which is protected with methods that do not permit an individual to concurrently obtain and use the electronic BCSI, is not provisioned access to electronic BCSI. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.
5. The SDT considered industry comments about defining the word "access". "Access" is broadly used across both the CIP and Operations & Planning Standards (e.g., open access) and carries different meanings in different contexts. Therefore, the SDT chose not to define "access" in the NERC Glossary of Terms. Instead, the SDT used the adjective "provisioned" to add context, thereby scoping CIP-004-X, Requirement R6. Do you agree the adjective "provisioned" in conjunction with the "Note" clarifies what "provisioned access" is? If not, please provide the basis for your disagreement and an alternate proposal.
6. In response to industry concerns regarding double jeopardy or confusion with CIP-013, the SDT removed CIP-011-X, Requirement R1 Parts 1.3 and 1.4, in favor of simplifying CIP-011-X, Requirement R1 Part 1.1, and adjusting Part 1.2 to broaden the focus around the implementation of protective methods and secure handling methods to mitigate risks of compromising confidentiality. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.
7. The SDT extended the implementation plan to 24-months in an attempt to align with the Project 2016-02 modifications that are on the same drafting timeline, and added an optional provision for early adoption. Do you agree this approach gives industry adequate time to implement without encumbering entities who are planning to, or are already using, third-party solutions (e.g., cloud services) for BCSI? If not, please provide the basis for your disagreement and an alternate proposal

**8. In looking at all proposed recommendations from the standard drafting team, are the proposed changes a cost-effective approach?**

**9. Please provide any additional comments for the SDT to consider, if desired.**

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Midcontinent ISO, Inc.	Bobbi Welch	2	MRO,RF,SERC	ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)	Ali Miremadi	CAISO	2	WECC
					Brandon Gleason	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Bobbi Welch	MISO	2	RF
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Michael Del Viscio	PJM	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					Marc Donaldson	Tacoma Public Utilities (Tacoma, WA)	3	WECC

					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Nick Fogleman	Prairie Power Incorporated	1,3	SERC
					Amber Skillern	East Kentucky Power Cooperative	1	SERC
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		DTE Energy - DTE Electric	Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Southwest Power Pool, Inc. (RTO)	Kimberly Van Brimer	2	MRO,WECC	Southwest Power Pool Standards Review Group (SSRG)	Kim Van Brimer	SPP	2	MRO
					Jim Williams	SPP	2	MRO
					Matt Harward	SPP	2	MRO

					Shannon Mickens	SPP	2	MRO
					Alan Wahlstrom	SPP	2	MRO
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
					Mark Garza	FirstEnergy-FirstEnergy	4	RF
Duke Energy	Masunch Bussey	1,3,5,6	FRCC,MRO,RF,SERC,Texas RE	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
					Lee Schuster	Duke Energy	3	SERC
Public Utility District No. 1 of Chelan County	Meaghan Connell	5		CHPD	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Ginette Lacasse	Public Utility District No. 1 of Chelan County	1	WECC
					Glen Pruitt	Public Utility District No. 1 of Chelan County	6	WECC
					Meaghan Connell	Public Utility District No. 1 Chelan County	5	WECC
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC

					James Mearns	Pacific Gas and Electric Company	5	WECC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Jim Howell	Southern Company - Southern Company Services, Inc. - Gen	5	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Helen Lainis	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen	5	NPCC

	Engineered Solutions International Inc.		
Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Shivaz Chopra	New York Power Authority	5	NPCC
Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
Nurul Abser	NB Power Corporation	1	NPCC
Randy MacDonald	NB Power Corporation	2	NPCC
Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
Vijay Puran	NYSPS	6	NPCC
ALAN ADAMSON	New York State Reliability Council	10	NPCC
Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC

					Brian Robinson	Utility Services	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Jim Grant	NYISO	2	NPCC
					John Pearson	ISONE	2	NPCC
					John Hastings	National Grid USA	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro-Quebec	2	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	6	SPP RE	OKGE	Sing Tay	OGE Energy - Oklahoma	6	MRO
					Terri Pyle	OGE Energy - Oklahoma	1	MRO

						Gas and Electric Co.		
					Donald Hargrove	OGE Energy - Oklahoma Gas and Electric Co.	3	MRO
					Patrick Wells	OGE Energy - Oklahoma Gas and Electric Co.	5	MRO
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC

1. The standards drafting team (SDT) considered industry's concerns about the phrase "provisioning of access" requesting clarity on this terminology. The SDT added "authorize, verify, and revoke provisioned access" to the parent requirement CIP-004-X, Requirement R6, and changed "provisioning of access" to "provisioned access" in the requirement parts. This should clarify the intent that it is a noun which scopes what the Registered Entity must authorize, verify, and revoke, rather than a verb relating to how provisioning should occur. That is up to the entity to determine. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer No

Document Name

Comment

The use of provisioned access is not addressed in CIP-004-X Requirement 5. The CIP-004-X requirements should use consistent terminology.

Likes 0

Dislikes 0

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer No

Document Name [2019-02\\_Unofficial\\_Comment\\_Form\\_03252021\\_Information-Protection-NSRF-draft-1\\_JC.docx](#)

Comment

**Comments:** WAPA believes the SDT is moving in the correct direction from the past version. WAPA does not support the term "provisioned access" as it is a non-definable term which has the potential to confuse regulators (auditors, risk, enforcement, FERC, NERC, etc...) and industry. The term also does not address the requirements in the SAR for entities storing BCSI off-prem (such as cloud data centers).

"Provisioned access" creates a security loophole whereas entities only require authorization for a provisioned access. For example, if access to BCSI is not provisioned, no authorization to BCSI is required. This does not meet the goal of SAR for controlling access to BCSI. Given the R6 definition whereas "access to BCSI" occurs when an individual has both "the ability to obtain and use BCSI," we recommend changing "provisioned access" to "access" that ensures only authorized individual can possess BCSI.

The use of "provisioned, provision or provisioning" of "access," regardless of tense, would require entities to be audited to, maintain, and provide documented lists of people and the "provisioned" configurations of entity BES Cyber System Information repositories in order to "verify" the "authorization" of such provisioned access.

The Measures section highlights this expectation where evidence may include individual records, or lists of whom is authorized. To achieve this evidence, entities would need to provide evidence of systems accounts of on-premises or off premises system repositories of BCSI. Cloud providers may not provide such lists of personnel who have administrative level access to cloud BCSI server repositories and entities will be unable to verify what 3rd party off-prem systems administrators have access to BCSI without litigation, yet entities will be asked to provide this information for an entire audit cycle

**Recommendations:**

1. Focus only on addressing electronic and physical access to BCSI in off-prem or cloud situations.
2. Consider the following language for R6 Part 6.1:

Authorize access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances. Access to BCSI includes:

6.1.1. Electronic access to electronic BCSI;

6.1.2 Physical access to physical BCSI;

6.1.3 Physical access to unencrypted electronic BCSI (See our comments in Q4).

3. Consider using the perspective of language in CIP-011 “ to prevent unauthorized access to BES Cyber System Information.” This allows entities to determine the risk and methods to protect BCSI

4. WAPA recommends addressing the two potential controls for access to off-prem BCS, 1) encrypting BCSI or 2) purchasing services which allow the entity to manage the off-prem authentication systems – thereby preventing 3rd party systems administrators or others from compromising entity BCSI stored in cloud data centers. This could be as simple as:

Implement at least one control to authorize access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances. Access to BCSI includes:

6.1.1. Electronic access to electronic BCSI;

6.1.2 Physical access to physical BCSI;

6.1.3 Physical access to unencrypted electronic BCSI (See our comments in Q4).

Likes 0

Dislikes 0

**Response**

**Dennis Sismaet - Northern California Power Agency - 6**

**Answer** No

**Document Name**

**Comment**

Please reference Marty Hostler's comments. Thanks.

Likes 0

Dislikes 0

**Response**

**JT Kuehne - AEP - 6****Answer** No**Document Name****Comment**

In AEP’s opinion, the updated language leaves room for interpretation. It might be simplistic to refer to the subparts of R6 instead of using specific words from the subparts.

The updated Requirement 6 would read: “Each Responsible Entity shall implement one or more documented access management program(s) to *meet subparts of R6 for provisioned access* to 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 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].”*

Likes 0

Dislikes 0

**Response****Bruce Reimer - Manitoba Hydro - 1****Answer** No**Document Name****Comment**

We disagree with “provisioned access” since there is a security concern where it only requires authorization for a provisioned access. If an access to BCSI is not provisioned, it means no authorization is required. This doesn’t meet the goal of SAR for controlling access to BCSI. Given that R6 has defined “access to BCSI” as an individual has both the ability to obtain and use BCSI, we suggest changing “provisioned access” to “access” that ensures only authorized individual can possess the BCSI. Also “unless already authorized according to Part 4.1” should be removed as having authorized access to CIP Cyber Assets does not preclude the authorization for having access to BCSI.

**Recommendations:**

We have the following suggested language for R6 Part 6.1:

Authorize access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances. Access to BCSI includes:

6.1.1. Electronic access to electronic BCSI;

6.1.2 Physical access to physical BCSI;

6.1.3 Physical access to unencrypted electronic BCSI (See our comments in Q4).

Likes 0

Dislikes 0

**Response**

**Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power**

**Answer** No

**Document Name**

**Comment**

Providing the definition of "provisioned access" within the Standard via the Note: within CIP-004 R6 Part 6.1 does not provide sufficient clarity to Industry. Tacoma Power suggests that it would be beneficial to create a NERC Glossary defined term for "Provisioned Access."

Likes 1 Snohomish County PUD No. 1, 3, Chaney Holly

Dislikes 0

**Response**

**Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP**

**Answer** No

**Document Name**

**Comment**

&bull;"Prior to provisioning, authorize **provisioned** access"? Wouldn't it be more appropriate to remove "provisioned" in 6.1.1 and 6.1.2? How can an entity authorize provisioned access if it hasn't been provisioned yet?

&bull; R6 requires provisioned access to BCSI to be authorized based on need, reviewed, and revoked upon a termination action.

&bull; R6 makes no mention of "Transfers or reassignments". R5 does not address revoking provisioned access to BCSI either, therefore entities are not required to revoke provisioned access to BCSI unless they are terminated.

&bull; Provisioned access to BCSI does not require an individual to have Cyber Security Awareness training or a PRA. Could an individual have no access to a BCS but have all of the information relating to the BCS.

&bull;In the Note section of R6.1 "Provisioned access is to be considered the result of the specific actions taken to provide an individual the means to access BCSI (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys)."

{C}- Recommend changing the e.g., section to read "physical keys or access control key cards, user accounts and associated rights and privileges, encryption keys).

Likes 0

Dislikes 0

**Response**

**Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations**

**Answer** No

**Document Name**

**Comment**

While the SDT did well in clarifying the intent of the provisioning, we do not feel a "Note" inserted into the requirement is sufficient to serve as a NERC definition. See Q5 comments.

Likes 0

Dislikes 0

**Response**

**Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1**

**Answer** No

**Document Name**

**Comment**

While the SDT did well in clarifying the intent of the provisioning, we do not feel a "Note" inserted into the requirement is sufficient to serve as a NERC definition. See Q5 comments.

AEPC has signed on to ACES comments.

Likes 0

Dislikes 0

**Response**

**Thomas Standifur - Austin Energy - 1,3,4,5,6**

**Answer** No

**Document Name** [TPWR\\_2019-02\\_Unofficial\\_Comment\\_Form\\_2021-05-10.docx20210504-17090-hsevrj.docx](#)

**Comment**

In support of Tacoma Powers' comments. Attached.

Likes 0

Dislikes 0

**Response**

**Benjamin Winslett - Georgia System Operations Corporation - 4****Answer** No**Document Name** [2019-02\\_Unofficial\\_Comment\\_Form\\_Final Draft.docx](#)**Comment**

For the purposes of providing for cloud storage and processing of BCSI information, the proposed changes are sufficient to provide for its use. However, the changes are silent with regard to the authorized incidental access of BCSI in a physical environment such as a meeting. It is recommended that clarification be provided in the requirement language for such circumstances. This is addressed in the Technical Rationale: however, it was not included in the standard.

The following modification is suggested to the Note in requirement part 6.1:

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). Provisioned access does not include temporary or incidental access when a specific mechanism for provisioning access is not available or feasible such as when an individual is given, merely views, or might see BCSI such as during a meeting or visiting a PSP, or when the BCSI is temporarily or incidentally located or stored on work stations, laptops, flash drives, portable equipment, offices, vehicles, etc.

Likes 1 Georgia Transmission Corporation, 1, Davis Greg

Dislikes 0

**Response****Gladys DeLaO - CPS Energy - 1,3,5****Answer** No**Document Name****Comment**

Part 6.1 perhaps should read as follows:

Unless already authorized according to Part 4.1, authorize provisioned access based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

CPS Energy suggests creating a NERC Glossary defined term for "Provisioned Access" instead of adding the Note: within CIP-004 R6 Part 6.1. Additionally, "obtain and use" should be included in the definition.

Likes 0

Dislikes 0

**Response****Michael Brytowski - Great River Energy - 1,3,5,6**

Answer	No
Document Name	
<p data-bbox="153 100 1957 155"><b>Comment</b></p> <p data-bbox="153 183 1957 305">The term “provisioned access” adds another undefined term to the NERC standards and doesn’t provide a clear path to regulatory off-prem or cloud data center services as proposed in the SAR. The only methods to control access to off-prem (cloud) BCSI is either by 1) encrypting BCSI or 2) purchasing services which allow the entity to manage the off-prem authentication systems – thereby preventing 3rd party systems administrators or others from compromising entity BCSI stored in cloud data centers. Option 2 is highly unlikely.</p> <p data-bbox="153 334 1957 451">a. “Provisioned access” creates a security loophole whereas entities only require authorization for a provisioned access. For example, if access to BCSI is not provisioned, no authorization to BCSI is required. This does not meet the goal of SAR for controlling access to BCSI. Given the R6 definition whereas “access to BCSI” occurs when an individual has both “the ability to obtain and use BCSI,” we recommend changing “provisioned access” to “access to BCSI”.</p> <p data-bbox="153 480 1957 540">b. The term “unless already authorized according to Part 4.1” should be removed. Why? Because having authorized access to CIP Cyber Assets does not preclude the authorization for having access to BCSI.</p> <p data-bbox="153 570 1957 781">c. The use of “provisioned, provision or provisioning” of “access,” regardless of tense, would require entities to be audited to, maintain, and provide documented lists of people and the “provisioned” configurations of entity BES Cyber System Information repositories in order to “verify” the “authorization” of such provisioned access. The Measures section highlights this expectation where evidence may include individual records, or lists of whom is authorized. To achieve this evidence, entities would need to provide evidence of systems accounts of on-premises or off premises system repositories of BCSI. Cloud providers will not provide such lists of personnel who have administrative level access to cloud BCSI server repositories and entities will be unable to verify what 3rd party off-prem systems administrators have access to BCSI, yet entities will be asked to provide this information for an entire audit cycle</p> <p data-bbox="153 810 1957 870">d. The current language requiring entities to 1) identify repositories and 2) authorize access based on need can also work for 3rd party off-prem or cloud locations without requiring lists of personnel or configurations of systems accounts for repositories of BCSI. (see recommendations)</p> <p data-bbox="153 899 390 927">Recommendations:</p> <ol data-bbox="153 956 1328 1040" style="list-style-type: none"> <li data-bbox="153 956 1328 984">1. Focus only on addressing electronic and physical access to BCSI in off-prem or cloud situations.</li> <li data-bbox="153 1013 761 1040">2. Consider the following language for R6 Part 6.1:</li> </ol> <p data-bbox="153 1070 1856 1130">Authorize access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances. Access to BCSI includes:</p> <ol data-bbox="153 1159 1123 1300" style="list-style-type: none"> <li data-bbox="153 1159 674 1187">6.1.1. Electronic access to electronic BCSI;</li> <li data-bbox="153 1216 631 1243">6.1.2 Physical access to physical BCSI;</li> <li data-bbox="153 1273 1123 1300">6.1.3 Physical access to unencrypted electronic BCSI (See our comments in Q4).</li> </ol> <ol data-bbox="153 1330 1920 1446" style="list-style-type: none"> <li data-bbox="153 1330 1920 1390">3. Consider using the perspective of language in CIP-011 “ to prevent unauthorized access to BES Cyber System Information.” This allows entities to determine the risk and methods to protect BCSI</li> <li data-bbox="153 1419 1813 1446">4. Consider using “authentication systems or encryption of BCSI” for personnel accessing electronic BCSI on cloud prem providers locations</li> </ol>	
Likes	0
Dislikes	0

<b>Response</b>	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<p>N&amp;ST notes that words can only be nouns, verbs, adjectives, etc. on an individual basis. Calling any two-word phrase a noun is grammatically incorrect. Beyond that, the phrase, "provisioned access," as used in proposed CIP-004 requirements, is itself grammatically incorrect by virtue of the fact "provisioned" is the past tense of the verb, "provision." It is not an adjective. An individual can be given access or can be provisioned access but cannot be given provisioned access. Since the SDT has adopted NERC's informal definition of "access to BCSI" as the ability to "obtain and use" it, N&amp;ST suggests the SDT maintain consistency with existing CIP-004 language and continue to require that Responsible Entities authorize access to BCSI (or BCSI storage locations), dropping the misunderstood and grammatically incorrect "provisioned access."</p>	
Likes	0
Dislikes	0
<b>Response</b>	
Donna Wood - Tri-State G and T Association, Inc. - 1	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
<p>Tri-State Generation and Transmission appreciates the time and effort given to this project and agrees with the revisions/changes.</p>	
Likes	0
Dislikes	0
<b>Response</b>	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
<p>Duke Energy agrees with the proposed change to "provisioned access" and that the entity will determine how that provisioning will occur.</p>	
Likes	0

Dislikes 0

**Response**

**Marty Hostler - Northern California Power Agency - 3,4,5,6**

**Answer** Yes

**Document Name**

**Comment**

NO. See WAPA and Indiana Comments

Likes 1 Northern California Power Agency, 6, Sismaet Dennis

Dislikes 0

**Response**

**Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman**

**Answer** Yes

**Document Name**

**Comment**

MPC agrees that this change provides greater clarity regarding the intent of this requirement and understands that it is the provisioned access that must be authorized, verified, and revoked.

Likes 0

Dislikes 0

**Response**

**Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6**

**Answer** Yes

**Document Name** [EEI Near Final Draft Comments\\_ Project 2019-02\\_Rev\\_0f\\_For Review FOR MEMBER REVIEW.docx](#)

**Comment**

OG&E agrees with EEI's comments

Likes 0

Dislikes 0

**Response**

**Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE**

**Answer** Yes

**Document Name**

**Comment**

OKGE supports comments provided by EEI.

Likes 0

Dislikes 0

**Response**

**Dan Bamber - ATCO Electric - 1**

**Answer** Yes

**Document Name**

**Comment**

Assuming that “provisioned access” means when someone gains and keeps BCSi access? Meaning if someone sees (screen sharing in view mode only) does not fall under “provisioned access”?

Likes 0

Dislikes 0

**Response**

**Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3**

**Answer** Yes

**Document Name**

**Comment**

Move the note to the parent requirement (R6), since it applies to more than 6.1, and remove the word “Note.”

Likes 0

Dislikes 0

**Response**

**Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments**

**Answer** Yes

**Document Name**

**Comment**

PG&E agrees with the proposed modifications. PG&E will define what is “provisioning of access” for our environment and will not need a defined NERC term since a NERC term may not cover all possible conditions for PG&E.

Likes 0

Dislikes 0

**Response**

**Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1**

**Answer** Yes

**Document Name**

**Comment**

Move the note to the parent requirement (R6), since it applies to more than 6.1, and remove the word “Note.”

Likes 0

Dislikes 0

**Response**

**Thomas Breene - WEC Energy Group, Inc. - 3**

**Answer** Yes

**Document Name**

**Comment**

We support EEI comments.

Likes 0

Dislikes 0

**Response**

**David Hathaway - WEC Energy Group, Inc. - 6**

**Answer** Yes

**Document Name**

**Comment**

Support comments made by EEI.

Likes 0

Dislikes 0

**Response**

**Clarice Zellmer - WEC Energy Group, Inc. - 5**

**Answer** Yes

**Document Name**

**Comment**

Agree with the proposed change. Would like the SDT to incorporate EEI comments as a non-substantive change during the final EEI review.

Likes 0

Dislikes 0

**Response**

**Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company**

**Answer** Yes

**Document Name**

**Comment**

Southern agrees as with EEI that the change provides greater clarity regarding the intent of the Requirement.

Likes 0

Dislikes 0

**Response**

**Daniel Gacek - Exelon - 1**

**Answer** Yes

<b>Document Name</b>	
<b>Comment</b>	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>John Galloway - ISO New England, Inc. - 2 - NPCC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
ISO New England supports this change.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Kinte Whitehead - Exelon - 3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Cynthia Lee - Exelon - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	

**Comment**

Exelon has elected to align with EEI in response to this question.

Likes 0

Dislikes 0

**Response****Becky Webb - Exelon - 6**

**Answer**

Yes

**Document Name**

**Comment**

Exelon has elected to align with EEI in response to this question.

Likes 0

Dislikes 0

**Response****Joshua Andersen - Salt River Project - 1,3,5,6 - WECC**

**Answer**

Yes

**Document Name**

**Comment**

Be careful adding "NOTES" to requirements. If the purpose is to increase clarity, then consider re-writing the requirement to improve clarify. NOTES may become overused across CIP standards and cause confusion.

Likes 0

Dislikes 0

**Response****Leonard Kula - Independent Electricity System Operator - 2**

**Answer**

Yes

**Document Name**

**Comment**

IESO supports the comments submitted by NPCC.

Likes 0

Dislikes 0

**Response**

**Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee**

**Answer** Yes

**Document Name**

**Comment**

We support these changes.

Likes 0

Dislikes 0

**Response**

**Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE**

**Answer** Yes

**Document Name**

**Comment**

CenterPoint Energy Houston Electric, LLC (CEHE) agrees that “provisioned access” is an improvement and supports the proposed change.

Likes 0

Dislikes 0

**Response**

**Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer**

**Answer** Yes

**Document Name**

**Comment**

Evergy supports and endorses the comments filed by the Edison Electric Institute.

Likes 0

Dislikes 0

**Response**

**Kevin Salsbury - Berkshire Hathaway - NV Energy - 5**

**Answer**

Yes

**Document Name**

**Comment**

NV Energy agrees that this change provides greater clarity regarding the intent of this Requirement.

Likes 0

Dislikes 0

**Response**

**Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2**

**Answer**

Yes

**Document Name**

**Comment**

None.

Likes 0

Dislikes 0

**Response**

**Constantin Chitescu - Ontario Power Generation Inc. - 5**

**Answer**

Yes

**Document Name**

**Comment**

OPG supports NPCC Regional Standards Committee's comments.

Likes 0

Dislikes 0

**Response**

**Larry Heckert - Alliant Energy Corporation Services, Inc. - 4**

**Answer** Yes

**Document Name**

**Comment**

Alliant Energy supports comments submitted by EEI.

Likes 0

Dislikes 0

**Response**

**Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)**

**Answer** Yes

**Document Name**

**Comment**

The ISO/RTO Council Standards Review Committee (IRC SRC) acknowledges the SDT for addressing our prior concerns surrounding the lack of clarity associated with "provision of access."

Likes 0

Dislikes 0

**Response**

**Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott**

**Answer** Yes

**Document Name**

**Comment**

ITC supports the response submitted by EEI

Likes 0

Dislikes 0

**Response**

**Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6**

**Answer** Yes

**Document Name**

**Comment**

PAC requests the SDT provide better definition of “provisioned access” than what was currently provided in Part 6.1

Likes 0

Dislikes 0

**Response**

**Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable**

**Answer** Yes

**Document Name**

**Comment**

EI agrees that this change provides greater clarity regarding the intent of this Requirement. However, use of the term “note” creates ambiguity because it is not clear whether the language in the note creates mandatory obligations. The use of the word “note” should be removed and the language contained in the note in Requirement R6, Part 6.1 should be elevated to the parent Requirement R6 because the term “provisioned access” is used in other parts of Requirement R6. Additionally, the note language should be strengthened for additional clarity (e.g., “is to be considered” may not be clear for industry to understand what the note means)

Likes 0

Dislikes 0

**Response**

**Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD**

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>LaTroy Brumfield - American Transmission Company, LLC - 1</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0

**Response**

**Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**William Steiner - Midwest Reliability Organization - 10**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Anthony Jablonski - ReliabilityFirst - 10**

**Answer**

Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>David Jendras - Ameren - Ameren Services - 3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	

**Response**

**Gail Golden - Entergy - Entergy Services, Inc. - 5**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Chris Carnesi - Northern California Power Agency - 3,4,5,6 - WECC**

**Answer**

**Document Name**

**Comment**

disregard

Likes 0

Dislikes 0

**Response**

**Rachel Coyne - Texas Reliability Entity, Inc. - 10**

**Answer**

<b>Document Name</b>	
<b>Comment</b>	
Texas RE seeks clarification regarding the scope of the revised CIP-004, Part 6.1. Specifically, Texas RE interprets “provisioned access” to include all instances in which an individual is “provisioned access” to BCSI. Accordingly, accidental or mistaken provisioned access would be within the scope of the requirement. Conversely, compromise of BCSI without any specific entity actions to provide the means to access BCSI (such as a data breach) would not be within the scope of the proposed requirement. Texas RE inquires as to whether this is the SDT’s intent.	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Doug Peterchuck - Omaha Public Power District - 1</b>	
<b>Answer</b>	
<b>Document Name</b>	<a href="#">2019-02_Unofficial_Comment_Form_Information-Protection-OPPD.docx</a>
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	

2. The SDT considered industry’s concerns about the absence of “obtain and use” language from the CMEP Practice Guide, which currently provides alignment on a clear two-pronged test of what constitutes access in the context of utilizing third-party solutions (e.g., cloud services) for BCSI. The SDT mindfully mirrored this language to assure future enforceable standards are not reintroducing a gap. Do you agree this clarifying language makes it clear both parameters of this two-pronged test for “obtain and use” must be met to constitute “access” to BCSI? If not, please provide the basis for your disagreement and an alternate proposal.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer No

Document Name

Comment

Please provide additional clarification in the Standard, and in the technical rationale.

Does the term, ‘use’ allow a user to unencrypt? Potential here for resulting in a potential data manipulation.

Recommendation:

Only use the term, “access.”

See the new R6 versus the former R4 language changes for clarification.

Likes 0

Dislikes 0

Response

Michael Brytowski - Great River Energy - 1,3,5,6

Answer No

Document Name

Comment

GRE agrees to adding “obtain and use” language to clarify what constitutes an access to BCSI, but disagree to the use of “provisioned access”. After clarifying the access to BCSI, the language “provisioned” should be removed since it has a security flaw and requires extensive records from repositories of BCSI (See our comments in Q1).

Recommendations:

1. Only use the term “access” as recommended in Q1

Likes 0

Dislikes 0

Response

<b>Gladys DeLaO - CPS Energy - 1,3,5</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
CPS Energy suggests "obtain and use" be included within R6 statement.	
"Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access <b>that grants the ability to obtain and use</b> BCSI pertaining to the "Applicable Systems" identified in CIP-004-X Table R6 – Access Management for BES Cyber System Information.	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Additional clarity is needed for what constitutes access by "obtain and use". Specifically, clarify what "use" means by defining the point at which information is considered "used". Does "use" mean immediately when the information is read by someone, or does it mean when the information is applied for some purpose? For example, if someone obtains information and can read it, and there are additional physical or electronic controls in place to prevent unauthorized use of the obtained information, do those controls then prevent "access to BCSI" based on the premise that information must be obtained and used to constitute access to BCSI?	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Thomas Standifur - Austin Energy - 1,3,4,5,6</b>	
<b>Answer</b>	No
<b>Document Name</b>	<a href="#">TPWR_2019-02_Unofficial_Comment_Form_2021-05-10.docx</a> <a href="#">20210504-17090-hsevrj.docx</a>
<b>Comment</b>	
In support of Tacoma Powers' comments. Attached.	
Likes	0

Dislikes 0

**Response**

**Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP**

**Answer** No

**Document Name**

**Comment**

Integrity should also be included as a security objective for BCSI in addition to confidentiality. Removing “obtain and use” is not consistent with the ERO Enterprise CMEP Practice Guide nor is it consistent with

[https://www.nerc.com/pa/comp/guidance/CMEPPPracticeGuidesDL/ERO%20Enterprise%20CMEP%20Practice%20Guide%20\\_%20BCSI%20-%20v0.2%20CLEAN.pdf](https://www.nerc.com/pa/comp/guidance/CMEPPPracticeGuidesDL/ERO%20Enterprise%20CMEP%20Practice%20Guide%20_%20BCSI%20-%20v0.2%20CLEAN.pdf)

In the R6 Requirement language "To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI."

- This statement contradicts the Requirement of R6.1. If a user must concurrently have the ability to both, obtain and use BCSI how does that provide the entity the ability to authorize based on need, as determined by the Responsible Entity?

- The webinar on 4/27/2021 attempted to clarify what the right and left lateral limits of BCSI “use” could be, but further clarifications might be needed to ensure a consistent approach is expected for authorization and provisioning.

Likes 0

Dislikes 0

**Response**

**Joshua Andersen - Salt River Project - 1,3,5,6 - WECC**

**Answer** No

**Document Name**

**Comment**

Access needs to be better defined, in particular the phrase “use BCSI” – being able to view a document or taking advantage of the information in the document. Is it “I have access to the file but not able to open it”, or is it “I have BES cyber system IP address, but no ability to get to those systems because there are other controls preventing me from using that information”?

Where is it in the standard that this is spelled out as a clear definition – “two-prong test”? This is not clear in the question above – shouldn’t the requirement be more clear?

Likes 0

Dislikes 0

**Response**

**Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power**

**Answer**

No

**Document Name**

**Comment**

The placement of the “obtain and use” statement gets lost within the construct of the Requirement Language, it appears as an add-on to the high level R6 language.

Suggested alternative:

“Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke the provisioned access that grants the ability to obtain and use 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 Table R6 – Access Management for BES Cyber System Information. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]”

Likes 1

Snohomish County PUD No. 1, 3, Chaney Holly

Dislikes 0

**Response**

**Bruce Reimer - Manitoba Hydro - 1**

**Answer**

No

**Document Name**

**Comment**

We agree to adding “obtain and use” language to clarify what constitutes an access to BCSI, but disagree to “provisioned access”. After clarifying the access to BCSI, the language “provisioned” should be removed since it has a security flaw (See our comments in Q1).

Likes 0

Dislikes 0

**Response**

**Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion**

**Answer**

No

**Document Name**

**Comment**

Dominion Energy is of the opinion that the terms “obtain and use” are ambiguous. We suggest additional language that provides for the Registered Entity to have the flexibility to define how these terms are applied by adding some additional language to the proposed Requirement as follows: *...an individual has both the ability to obtain and use BCSI as defined by the Registered Entity.*

Likes 0

Dislikes 0

**Response****Dennis Sismaet - Northern California Power Agency - 6**

**Answer**

No

**Document Name**

**Comment**

Please reference Marty Hostler's comments. Thanks.

Likes 0

Dislikes 0

**Response****Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones**

**Answer**

No

**Document Name**

**Comment**

1. We agree to adding “obtain and use” language to clarify what constitutes an access to BCSI, but disagree to the use of “provisioned access”. After clarifying the access to BCSI, the language “provisioned” should be removed since it has a security flaw and requires extensive records from repositories of BCSI (See our comments in Q1).

**Recommendations:**

1. Only use the term “access” as recommended in Q1

Likes 0

Dislikes 0

**Response**

**Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1****Answer** No**Document Name****Comment**

A user can have provisioned access to obtain BCSI and not use it. The Registered Entity is currently receiving an authorization for a user based on need to access BCSI. Access to BCSI is enough to constitute an authorization regardless of use. While this clarification assists in the context of third-party solutions it does not provide clarity for electronic or physical access to BCSI.

Likes 0

Dislikes 0

**Response****Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable****Answer** Yes**Document Name****Comment**

EEI agrees that the clarifying language contained in the two-prong test (i.e., “obtain and use”) provides reasonable protections for controlling access to BCSI, particularly as it relates to BCSI that might be stored in a third-party cloud environment. EEI also agrees that having physical access to BCSI but not having the ability to use it is impractical because it does not represent access from a functional standpoint or for a useful purpose.

Likes 0

Dislikes 0

**Response****Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC****Answer** Yes**Document Name****Comment**

Black Hills would recommend that 6.1’s “Note” section use the same language as R6 opening paragraph. Specifically “ability to obtain and use” should be used whenever possible, in this instance the “Note” section may read like this, “Provisioned access is to be considered the result of the specific actions resulting in an individual’s ability to obtain and use BCSI.”

Likes 0

Dislikes 0

**Response**

**Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott**

**Answer** Yes

**Document Name**

**Comment**

ITC supports the response submitted by EEI

Likes 0

Dislikes 0

**Response**

**Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)**

**Answer** Yes

**Document Name**

**Comment**

The IRC SRC supports the reinstatement of "obtain and use" concepts.

Likes 0

Dislikes 0

**Response**

**Larry Heckert - Alliant Energy Corporation Services, Inc. - 4**

**Answer** Yes

**Document Name**

**Comment**

Alliant Energy supports comments submitted by EEI.

Likes 0

Dislikes 0

**Response**

**Constantin Chitescu - Ontario Power Generation Inc. - 5**

**Answer** Yes

**Document Name**

**Comment**

OPG supports NPCC Regional Standards Committee's comments.

Likes 0

Dislikes 0

**Response**

**Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2**

**Answer** Yes

**Document Name**

**Comment**

None.

Likes 0

Dislikes 0

**Response**

**Kevin Salsbury - Berkshire Hathaway - NV Energy - 5**

**Answer** Yes

**Document Name**

**Comment**

NVE agrees that the clarifying language contained in the two-prong test (i.e., "obtain and use") provides reasonable protections for controlling access to BCSI, particularly as it relates to BCSI that might be stored in a third-party cloud environment. NVE also agrees that having physical access to BCSI but not having the ability to use it is impractical because it does not represent access from a functional standpoint or for a useful purpose.

Likes 0

Dislikes 0

**Response**

**Rachel Coyne - Texas Reliability Entity, Inc. - 10**

**Answer** Yes

**Document Name**

**Comment**

Texas RE agrees that the two-pronged test is an improvement over the existing language. Texas RE is concerned, however, that the verbiage “obtain and use” is subject to further interpretation. One approach could be to clarify the verbiage to read: *“the authorized ability to retrieve, modify, copy, or move BCSI”*. Alternatively, Texas RE recommends creating bright line criteria establishing what it means for the BCSI to be usable.

Likes 0

Dislikes 0

**Response**

**Benjamin Winslett - Georgia System Operations Corporation - 4**

**Answer** Yes

**Document Name**

**Comment**

The ‘obtain and use’ language introduced provides valuable clarification with regard to provisioning and deprovisioning of access and provides context that will enable clearly defined opportunities to leverage cloud services. However, as drafted, the standard effectively provides different explanations for “access” versus “provisioned access.” It would increase clarity if these explanations were combined. It is recommended that the note explaining provisioned access be moved to the main requirement so that all explanatory statements regarding access or provisioned access are in the same place. In this manner, it is clear that the clarifications to “provisioned access” apply across all parts of requirement R6.

Consistent with our recommendation to question 1 regarding incidental access, this would modify the main requirement of R6 as follows:

...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). Provisioned access does not include temporary or incidental access when a specific mechanism for provisioning access is not available or feasible such as when an individual is given, merely views, or might see BCSI such as during a meeting or visiting a PSP, or when the BCSI is temporarily or incidentally located or stored on work stations, laptops, flash drives, portable equipment, offices, vehicles etc.

Likes 1 Georgia Transmission Corporation, 1, Davis Greg

Dislikes 0

**Response**

**Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer**

**Answer** Yes

**Document Name**

**Comment**

Entergy supports and endorses the comments filed by the Edison Electric Institute.

Likes 0

Dislikes 0

**Response**

**Gail Golden - Entergy - Entergy Services, Inc. - 5**

**Answer** Yes

**Document Name**

**Comment**

*Entergy supports the inclusion of the “obtain and use” language from the CMEP Practice Guide. This language clarifies that users with “access” for purposes of the requirement must be able to obtain and use BCSI, which addresses industry’s concern regarding encrypted data. In particular, the prior language could present a grey area where a user could receive an encrypted BCSI item and be considered as having the BCSI even though they (conceivably) could not use it. This approach aligns with Entergy’s interpretation under both its current BCSI program, as well as the guidance and position we are pursuing for BCSI in the cloud*

Likes 0

Dislikes 0

**Response**

**Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1**

**Answer** Yes

**Document Name**

**Comment**

AEPC has signed on to ACES comments.

Likes 0

Dislikes 0

**Response**

**Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee**

**Answer** Yes

**Document Name**

**Comment**

We support the update to this Requirement language.

Likes 0

Dislikes 0

**Response****Leonard Kula - Independent Electricity System Operator - 2****Answer**

Yes

**Document Name****Comment**

Support the update to this Requirement language.

Likes 0

Dislikes 0

**Response****Becky Webb - Exelon - 6****Answer**

Yes

**Document Name****Comment**

Exelon has elected to align with EEI in response to this question.

Likes 0

Dislikes 0

**Response****Cynthia Lee - Exelon - 5****Answer**

Yes

**Document Name****Comment**

Exelon has elected to align with EEI in response to this question.

Likes 0

Dislikes 0

**Response**

**Kinte Whitehead - Exelon - 3**

**Answer**

Yes

**Document Name**

**Comment**

Exelon has elected to align with EEI in response to this question.

Likes 0

Dislikes 0

**Response**

**John Galloway - ISO New England, Inc. - 2 - NPCC**

**Answer**

Yes

**Document Name**

**Comment**

ISO New England supports this update.

Likes 0

Dislikes 0

**Response**

**Daniel Gacek - Exelon - 1**

**Answer**

Yes

**Document Name**

**Comment**

Exelon has elected to align with EEI in response to this question.

Likes 0

Dislikes 0

**Response**

**Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company**

**Answer**

Yes

**Document Name**

**Comment**

Southern agrees that for access to occur, a user must both obtain BCSI and possess the ability to use BCSI according to the CMEP dated April 26, 2019.

Likes 0

Dislikes 0

**Response**

**David Hathaway - WEC Energy Group, Inc. - 6**

**Answer**

Yes

**Document Name**

**Comment**

Support comments made by EEI.

Likes 0

Dislikes 0

**Response**

**Thomas Breene - WEC Energy Group, Inc. - 3**

**Answer**

Yes

**Document Name**

**Comment**

We support EEI comments.

Likes 0

Dislikes 0

**Response**

**Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments**

**Answer**

Yes

**Document Name**

**Comment**

PG&E agrees that the clarification is sufficient.

Likes 0

Dislikes 0

**Response**

**Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE**

**Answer**

Yes

**Document Name**

**Comment**

OKGE supports comments provided by EEI.

Likes 0

Dislikes 0

**Response**

**JT Kuehne - AEP - 6**

**Answer**

Yes

**Document Name**

**Comment**

AEP agrees with the addition of "obtain and use" language in R6 parent requirement, as this is in alignment with AEP's BCSInfo program.

Likes 0

Dislikes 0

<b>Response</b>	
<b>Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name</b> Southwest Power Pool Standards Review Group (SSRG)	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
The SPP Standards Review Group (SSRG) recommends the word “use” have clarity supplied around the term.	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
MPC appreciates the SDT’s efforts to include the concept from the CMEP Practice Guide. However, we would prefer the language be more specific to CIP-004, rather than re-introduce the broader “access” concept that goes beyond CIP-004 by using this language instead: “An individual is considered to have provisioned access to BCSI if they concurrently have the means to both obtain and use the BCSI (e.g., an individual who obtains encrypted BCSI but does not have the encryption keys does not have provisioned access).” The example is helpful in understanding what is meant by “obtain and use.”	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Marty Hostler - Northern California Power Agency - 3,4,5,6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
NO. See WAPA Contents.	
Likes	1
Dislikes	0
Northern California Power Agency, 6, Sismaet Dennis	

<b>Response</b>	
<b>Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Duke Energy agrees the proposed changes make it clear that both parameters of the two-pronged test for “obtain and use” must be met to constitute “access” to BCSI.	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3</b>	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>David Jendras - Ameren - Ameren Services - 3</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Clarice Zellmer - WEC Energy Group, Inc. - 5</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0

**Response**

**Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Dan Bamber - ATCO Electric - 1**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Anthony Jablonski - ReliabilityFirst - 10**

**Answer** Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>William Steiner - Midwest Reliability Organization - 10</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	

**Response**

**LaTroy Brumfield - American Transmission Company, LLC - 1**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority**

**Answer** Yes

**Document Name**

<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Donna Wood - Tri-State G and T Association, Inc. - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

3. The SDT considered industry comments regarding the removal of storage locations. The SDT must enable the CIP standards for the use of third-party solutions (e.g., cloud services) for BCSI, and retention of that language hinders meeting those FERC directives. The absence of this former language does not preclude an entity from defining storage locations as the method used within an entity's access management program. CIP-004-X, Requirement R6, is at an objective level to permit more than that one approach. Do you agree the requirement retains the flexibility for storage locations to be used as one way to meet the objective? If not, please provide the basis for your disagreement and an alternate proposal.

**Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1**

**Answer** No

**Document Name**

**Comment**

Storage locations identified for using BCSI is reference in CIP-011-X. CIP-004-X and CIP-011-X should provide consistent terminology.

Likes 0

Dislikes 0

**Response**

**Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones**

**Answer** No

**Document Name**

**Comment**

1.

- i. We agree to retaining the flexibility for storage locations to be used as one way to meet the objective of SAR, but disagree to using "provisioned access" (See our comments regarding "provisioned access" in Q1).
- ii. The requirement to provide lists of personnel with "provisioned access" would also require entities to identify the locations of BCSI and by auditors whom are required to make the link between the repository of BCSI which has been provisioned for access.

**Recommendation:**

Retain the current language and focus on auditable methods to protect BCSI at 3rd party off-prem (cloud) locations.

Likes 0

Dislikes 0

**Response**

**Dennis Sismaet - Northern California Power Agency - 6**

**Answer** No

<b>Document Name</b>	
<b>Comment</b>	
Please reference Marty Hostler's comments. Thanks.	
Likes	0
Dislikes	0
<b>Response</b>	
<b>JT Kuehne - AEP - 6</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<p>The currently effective Requirement Part 4.1.3 of CIP-004-6 reads, "Access to designated storage locations, whether physical or electronic, for BES Cyber System Information." Removing "storage locations" from R6 and its subparts, makes it difficult for the entities to comply, as the entities need to expand their searches for access control when providing compliance evidence. Similar to "Provisioned access" noun, simply stating "BCSI" will make it intangible where keeping "storage locations" will make the requirement and its subparts tangible.</p> <p>AEP understands the intent but it is not clear based on how it is currently worded. AEP requests SDT to provide further clarification on the intent and to provide better definition on "provisioned access" than what was currently provided in Part 6.1 ("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).") AEP also recommends SDT to focus on auditable methods to protect BCSI at 3rd party off-premise (cloud) locations.</p> <p>AEP currently defines what constitutes as storage locations in CIP-011-2 R1 information protection program, but for other smaller entities this may become further complicated to define besides managing access to BCSI storage locations.</p>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
To ensure a consistent understanding of the issues surrounding information storage on the cloud, Dominion Energy suggests using language similar to that in CIP-011 that addresses cloud storage in the proposed CIP-004.	

Likes 0

Dislikes 0

**Response**

**Bruce Reimer - Manitoba Hydro - 1**

**Answer** No

**Document Name**

**Comment**

We agree to retaining the flexibility for storage locations to be used as one way to meet the objective of SAR, but disagree to using “provisioned access” (See our comments regarding “provisioned access” in Q1). The objective of SAR and NERC CMEP BCSI guidance is to prevent unauthorized access to BCSI rather than “provisioned access to BCSI”. Using “provisioned access to BCSI is lowering the bar for the BCSI authorization doesn’t meet the goal of SAR for controlling unauthorized access to BCSI. Also “provisioned access” is subjective resulting in no audit consistency since the NERC entities and auditors may have different ways to interpret it.

Likes 0

Dislikes 0

**Response**

**Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power**

**Answer** No

**Document Name**

**Comment**

Tacoma Power supports the objective of the Project 2019-02 SAR, which includes providing a path to allow the use of modern third-party data storage and analysis systems. While the use of third-party data storage may be enabled to a degree with these modifications, the use of third-party analysis systems is likely not. Any managed security provider’s solution would likely be considered an EACMS based on the current EACMS definition, which carries a host of CIP Requirements, not the least of which are found in CIP-004, which would preclude the use of these services in almost every case. Additionally many modern cybersecurity tools such as local endpoint protection systems, now make use of Cloud services to provide additional context to the information seen on local systems, and require that much of the system log data be pushed to the Cloud to enable this analysis.

Tacoma Power suggests modification of the EACMS definition to split off access control from access monitoring, which then would allow for requirement applicability based on risk for access control systems versus access monitoring systems.

Likes 1

Snohomish County PUD No. 1, 3, Chaney Holly

Dislikes 0

**Response**

**Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations**

**Answer** No

**Document Name**

**Comment**

While we agree with the SDT retaining the flexibility for storage locations to be used as one way to meet the objective of SAR, we disagree with using "provisioned access" based on our concerns in Q5.

Likes 0

Dislikes 0

**Response**

**Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1**

**Answer** No

**Document Name**

**Comment**

While we agree with the SDT retaining the flexibility for storage locations to be used as one way to meet the objective of SAR, we disagree with using "provisioned access" based on our concerns in Q5.

AEPC has signed on to ACES comments.

Likes 0

Dislikes 0

**Response**

**Thomas Standifur - Austin Energy - 1,3,4,5,6**

**Answer** No

**Document Name** [TPWR\\_2019-02\\_Unofficial\\_Comment\\_Form\\_2021-05-10.docx20210504-17090-hsevrj.docx](#)

**Comment**

In support of Tacoma Powers' comments. Attached.

Likes 0

Dislikes 0

**Response**

**Kevin Salisbury - Berkshire Hathaway - NV Energy - 5****Answer** No**Document Name****Comment**

NVE agrees that the approach provides entities with the additional flexibility to develop and define their own internal procedures regardless of whether they are using off-premise storage or simply maintaining backward compatibility with their legacy systems. However, we also recognize that the removal of the term “storage locations” does present challenges for entities trying to reconcile internal processes for legacy systems. For this reason, we recommend the SDT provide greater clarity through Implementation Guidance, to assist those entities with developing effective processes resulting from these changes. Specifically, the SDT should develop guidance that would be useful in understanding how to define storage locations as a method within registered entities’ access management programs. Such guidance would be helpful to ensure backward compatibility.

Likes 0

Dislikes 0

**Response****Gladys DeLaO - CPS Energy - 1,3,5****Answer** No**Document Name****Comment**

CPS Energy suggests creating a NERC Glossary defined term for “Provisioned Access” instead of adding the Note: within CIP-004 R6 Part 6.1. Additionally, “obtain and use” should be included in the definition.

Likes 0

Dislikes 0

**Response****Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2****Answer** No**Document Name****Comment**

ERCOT hereby incorporates the comments filed by the ISO/RTO Council Standards Review Committee.

Likes 0

Dislikes 0

**Response**

**Michael Brytowski - Great River Energy - 1,3,5,6**

**Answer** No

**Document Name**

**Comment**

a. GRE agrees to retaining the flexibility for storage locations to be used as one way to meet the objective of SAR, but disagree to using “provisioned access” (See our comments regarding “provisioned access” in Q1).

b. The requirement to provide lists of personnel with “provisioned access” would also require entities to identify the locations of BCSI and by auditors whom are required to make the link between the repository of BCSI which has been provisioned for access.

Recommendation:

Retain the current language and focus on auditable methods to protect BCSI at 3rd party off-prem (cloud) locations.

Likes 0

Dislikes 0

**Response**

**Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)**

**Answer** No

**Document Name**

**Comment**

The IRC SRC is concerned that keeping “storage locations” without defining it in the standard or the NERC Glossary will require entities to define it for themselves. This will create a variety of interpretations throughout the regions.

The IRC SRC recommends the SDT consider defining the term “storage locations” to indicate that storage locations may be physical locations or virtual locations that are protected using technologies such as access control or encryption

Likes 0

Dislikes 0

**Response**

**Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh**

**Answer** No

**Document Name**

**Comment**

N&ST strongly disagrees with the SDT's assertion that retention of "designated storage locations," is a hindrance to using third party / cloud services, and notes that the SAR for this project states the project will provide "...a secure path towards utilization of modern third-party data storage and analysis systems." The real roadblock here, for which solutions are already available, is encryption key management (see our response to Question 9). In addition, N&ST is concerned that one or more Regional Entities may or may not agree with the SDT's frequently repeated promise that managing access to BSCI storage locations will be accepted as a fully compliant equivalent to managing access to BCSI, and that Responsible Entities have the option of maintaining current practices. As a compromise, N&ST recommends the proposed CIP-004 changes be amended to state explicitly that Responsible Entities must manage access to one or more of: BCSI, designated electronic storage locations, and designated physical storage locations. This change would give entities the flexibility of maintaining or dropping "storage locations" or perhaps implementing a hybrid approach.

Likes 0

Dislikes 0

**Response**

**Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6**

**Answer** No

**Document Name**

**Comment**

The currently effective Requirement Part 4.1.3 of CIP-004-6 reads, "Access to designated storage locations, whether physical or electronic, for BES Cyber System Information." The removal of, "storage locations" from R6 and its subparts, makes it difficult for the entities to comply, as the entities need to expand their searches for access control when providing compliance evidence.

We disagree with using, "provisioned access" as it is currently defined. The requirement to provide lists of personnel with "provisioned access" would also require entities to identify the locations of BCSI, and for auditors to make that link to the repository of BCSI, to determine which has been provisioned for access.

Similar to "Provisioned access" noun, simply stating "BCSI" will make it intangible where keeping "storage locations" will make the requirement and its subparts tangible. See Q1 comment.

Recommendation:

Retain the current language and focus on auditable methods to protect BCSI at third-party off-prem (*cloud based*) locations.

Use language similar to that in CIP-011 that addresses cloud storage for the proposed CIP-004.

Recommend creating a NERC Glossary defined term for "Provisioned Access."

Likes 0

Dislikes 0

**Response**

**Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy**

**Answer** Yes

<b>Document Name</b>	
<b>Comment</b>	
Duke Energy agrees the proposed changes retain the flexibility for storage locations to be used as one way to meet the objective.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
See comments in response to #9 below.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Marty Hostler - Northern California Power Agency - 3,4,5,6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
NO. See WAPA and Indianca Comments.	
Likes 1	Northern California Power Agency, 6, Sismaet Dennis
Dislikes 0	
<b>Response</b>	
<b>Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

MPC agrees that this approach provided entities with the flexibility to define their own internal procedures, which may include continuing to designate storage locations for BCSI to which individuals can have provisioned access. Provisioned access for those individuals can be authorized, verified, and revoked.

Likes 0

Dislikes 0

### Response

**Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE**

**Answer**

Yes

**Document Name**

**Comment**

OKGE supports comments provided by EEI.

Likes 0

Dislikes 0

### Response

**Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments**

**Answer**

Yes

**Document Name**

**Comment**

PG&E agrees with the modifications which make the Requirement more objective-based.

Likes 0

Dislikes 0

### Response

**Thomas Breene - WEC Energy Group, Inc. - 3**

**Answer**

Yes

**Document Name**

**Comment**

We support EEI comments.

Likes 0

Dislikes 0

**Response**

**David Hathaway - WEC Energy Group, Inc. - 6**

**Answer**

Yes

**Document Name**

**Comment**

Support comments made by EEI.

Likes 0

Dislikes 0

**Response**

**Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company**

**Answer**

Yes

**Document Name**

**Comment**

Southern agrees as with EEI and industry that this approach provided entities with the needed flexibility to develop and define their own internal procedures of what constitutes storage for current and future use.

Likes 0

Dislikes 0

**Response**

**Daniel Gacek - Exelon - 1**

**Answer**

Yes

**Document Name**

**Comment**

Exelon has elected to align with EEI in response to this question.

Likes 0

Dislikes 0

**Response**

**John Galloway - ISO New England, Inc. - 2 - NPCC**

**Answer**

Yes

**Document Name**

**Comment**

ISO New England supports this change.

Likes 0

Dislikes 0

**Response**

**Kinte Whitehead - Exelon - 3**

**Answer**

Yes

**Document Name**

**Comment**

Exelon has elected to align with EEI in response to this question.

Likes 0

Dislikes 0

**Response**

**Cynthia Lee - Exelon - 5**

**Answer**

Yes

**Document Name**

**Comment**

Exelon has elected to align with EEI in response to this question.

Likes 0

Dislikes 0

**Response**

**Becky Webb - Exelon - 6**

**Answer**

Yes

**Document Name**

**Comment**

Exelon has elected to align with EEI in response to this question.

Likes 0

Dislikes 0

**Response**

**Leonard Kula - Independent Electricity System Operator - 2**

**Answer**

Yes

**Document Name**

**Comment**

If the entity continues using storage location, the entity is responsible for defining storage location. Request confirmation of this expectation.

Likes 0

Dislikes 0

**Response**

**Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee**

**Answer**

Yes

**Document Name**

**Comment**

If the entity continues using storage location, the entity is responsible for defining storage location. Request confirmation of this expectation.

Likes 0

Dislikes 0

**Response**

**Gail Golden - Entergy - Entergy Services, Inc. - 5**

**Answer** Yes

**Document Name**

**Comment**

*An organization should be able to define storage locations as well as decommission them, as long as appropriate controls are applied in both processes. The revised standard allows entities to apply controls at either the data level or storage level, without requiring either so long as data security is achieved.*

Likes 0

Dislikes 0

**Response**

**Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer**

**Answer** Yes

**Document Name**

**Comment**

Evergy supports and endorses the comments filed by the Edison Electric Institute.

Likes 0

Dislikes 0

**Response**

**Benjamin Winslett - Georgia System Operations Corporation - 4**

**Answer** Yes

**Document Name**

**Comment**

Yes, this modification retains the flexibility for storage locations to be used as one way to meet the objective. However, absent clarifying language in the requirement regarding temporary and incidental access, the standard may inadvertently significantly expand the scope over the currently approved

standard. This language is included in the Technical Rationale, but is not included in any enforceable language. It is recommended that additional clarification be added as outlined in the response to questions 1 and 2.

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
---------	---

Dislikes 0	
------------	--

**Response**

**Constantin Chitescu - Ontario Power Generation Inc. - 5**

<b>Answer</b>	Yes
---------------	-----

<b>Document Name</b>	
----------------------	--

**Comment**

OPG supports NPCC Regional Standards Committee's comments.

Likes 0	
---------	--

Dislikes 0	
------------	--

**Response**

**Larry Heckert - Alliant Energy Corporation Services, Inc. - 4**

<b>Answer</b>	Yes
---------------	-----

<b>Document Name</b>	
----------------------	--

**Comment**

Alliant Energy supports comments submitted by EEI.

Likes 0	
---------	--

Dislikes 0	
------------	--

**Response**

**Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott**

<b>Answer</b>	Yes
---------------	-----

<b>Document Name</b>	
----------------------	--

**Comment**

ITC supports the response submitted by EEI

Likes 0

Dislikes 0

**Response**

**Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable**

**Answer**

Yes

**Document Name**

**Comment**

EEl agrees that the approach provides entities with the needed flexibility to develop and define their own internal procedures regardless of whether they are using off-premise storage or simply maintaining backward compatibility with their legacy systems. However, we also recognize that the removal of the term "storage locations" does present challenges for entities trying to reconcile internal processes for legacy systems. For this reason, we recommend the SDT provide greater clarity through Implementation Guidance, to assist those entities with developing effective processes resulting from these changes. Specifically, the SDT should develop guidance that would be useful in understanding how to define storage locations as a method within registered entities' access management programs. Such guidance would be helpful to ensure backward compatibility.

Likes 0

Dislikes 0

**Response**

**Donna Wood - Tri-State G and T Association, Inc. - 1**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**LaTroy Brumfield - American Transmission Company, LLC - 1**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter**

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>William Steiner - Midwest Reliability Organization - 10</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Anthony Jablonski - ReliabilityFirst - 10</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0

**Response**

**Dan Bamber - ATCO Electric - 1**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric**

**Answer**

Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Clarice Zellmer - WEC Energy Group, Inc. - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>David Jendras - Ameren - Ameren Services - 3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	

**Response**

**Joshua Andersen - Salt River Project - 1,3,5,6 - WECC**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Rachel Coyne - Texas Reliability Entity, Inc. - 10**

**Answer** Yes

**Document Name**

Comment	
Likes 0	
Dislikes 0	
Response	
<b>Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

4. To address industry comments while also enabling entities to use third-party solutions (e.g., cloud services) for BCSI, in CIP-004-X, Requirement R6 Part 6.1, the SDT made a distinction between “electronic access to electronic BCSI” versus “physical access to physical BCSI”. This clarifies physical access alone to hardware containing electronic BCSI, which is protected with methods that do not permit an individual to concurrently obtain and use the electronic BCSI, is not provisioned access to electronic BCSI. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

**Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC**

**Answer** No

**Document Name**

**Comment**

Black Hills does not find the distinction necessary. If consistent use of the language “obtain and use” then it should be evident that physical access to a computer, device, etc. does not constitute access to BCSI. The same logic that applies to a locked filing cabinet should apply to cyber access as well.

Likes 0

Dislikes 0

**Response**

**Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)**

**Answer** No

**Document Name**

**Comment**

The IRC SRC observes that this approach appears to compensate for the removal of the concept of BCSI repositories. We suggest changing “physical access to physical BCSI” to “physical access to physical BCSI **storage locations**” as “physical BCSI” limits the definition to the information itself (e.g. the drawings) and would not extend to include the protection of the storage location or repository as well (e.g. the drawer where the drawings are stored).

Likes 0

Dislikes 0

**Response**

**Michael Brytowski - Great River Energy - 1,3,5,6**

**Answer** No

**Document Name**

**Comment**

GRE disagrees that the physical access only applies to physical BCSI since controlling access to unencrypted BCSI has not been addressed but will be required for 3rd party off-prem (cloud) repositories. The physical access to Cyber Assets is a fast avenue to owning the unencrypted electronic BCSI it contains, which meets “obtain and use” condition and constitutes an access to BCSI.

Recommendation:

Adding “Physical access to unencrypted electronic BCSI” to R6 Part 6.1.3 (See our suggested R6 Part 6.1 changes in Q1).

Likes 0

Dislikes 0

### Response

**Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2**

Answer

No

Document Name

Comment

ERCOT hereby incorporates the comments filed by the ISO/RTO Council Standards Review Committee.

Likes 0

Dislikes 0

### Response

**Gladys DeLaO - CPS Energy - 1,3,5**

Answer

No

Document Name

Comment

CPS Energy disagrees with the proposed changes, including a statement for both physical and electronic access only leads to further questions. CPS Energy propose defining what is considered Physical BCSI and Electronic BCSI as those terms are not defined by NERC – although should be understood Physical BCSI could be BCSI on printed medium, white board scribbles, photograph and electronic BCSI would be word docs, pdf, text file, digital photos – each person could define or scope the words physical and electronic in different ways.

Likes 0

Dislikes 0

### Response

**Benjamin Winslett - Georgia System Operations Corporation - 4**

<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
It is recommended that the SDT directly clarify the understanding that access to data or a tangible item that contains information does not equate to access to that information. The addition of such a clarification in the standard would simplify the understanding of the applicability of controls to the protection of BCSI.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
<b>Response</b>	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
See our comments around "provisioned access" in Q5 AEPC has signed on to ACES comments.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
See our comments around "provisioned access" in Q5	
Likes 0	
Dislikes 0	
<b>Response</b>	

**Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3**

**Answer** No

**Document Name**

**Comment**

In the measures for R6.1, suggested evidence includes “the justification of business need for the provisioned access.” However, similar requirement 4.1 states “authorize based on need” but does not call out the justification of business need in the measures. 6.1 and 4.1 should be consistent in measures.

Likes 0

Dislikes 0

**Response**

**Bruce Reimer - Manitoba Hydro - 1**

**Answer** No

**Document Name**

**Comment**

We disagree that the physical access only applies to physical BCSI since the controlling access to unencrypted BCSI has not been addressed. The physical access to Cyber Assets is a fast avenue to owning the unencrypted electronic BCSI it contains, which meets “obtain and use” condition and constitutes an access to BCSI. We suggest adding “Physical access to unencrypted electronic BCSI” to R6 Part 6.1.3 (See our suggested R6 Part 6.1 changes in Q1).

Likes 0

Dislikes 0

**Response**

**Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion**

**Answer** No

**Document Name**

**Comment**

Dominion Energy is concerned the the SDT is attempting to define the term "provisioned access" in a footnote. Leaving a term open to interpretation across Standards is concerning and if a term is being used inconsistently it should be defined in the Glossary of Terms rather than through a footnote for a Standard.

Likes 0

Dislikes 0

**Response**

**JT Kuehne - AEP - 6**

**Answer** No

**Document Name**

**Comment**

“Physical BCSI” is not a defined term. AEP recommends SDT to either define “physical BCSI” or add further clarifications in Requirement 6. AEP recommends using the existing language, “*Access to designated storage locations, whether physical or electronic, for BES Cyber System Information*” under 6.1.

Likes 0

Dislikes 0

**Response**

**Dennis Sismaet - Northern California Power Agency - 6**

**Answer** No

**Document Name**

**Comment**

Please reference Marty Hostler's comments. Thanks.

Likes 0

Dislikes 0

**Response**

**Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones**

**Answer** No

**Document Name**

**Comment**

We disagree that the physical access only applies to physical BCSI since controlling access to unencrypted BCSI has not been addressed but will be required for 3rd party off-prem (cloud) repositories. The physical access to Cyber Assets is a fast avenue to owning the unencrypted electronic BCSI it contains, which meets “obtain and use” condition and constitutes an access to BCSI.

**Recommendation:**

Adding "Physical access to unencrypted electronic BCSI" to R6 Part 6.1.3 (See our suggested R6 Part 6.1 changes in Q1).

Likes 0

Dislikes 0

**Response**

**Marty Hostler - Northern California Power Agency - 3,4,5,6**

**Answer**

No

**Document Name**

**Comment**

NO. Cloud services should be allowed. However, there is no need to make a distinction between electronic access and physical access.

Likes 1

Northern California Power Agency, 6, Sismaet Dennis

Dislikes 0

**Response**

**Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1**

**Answer**

No

**Document Name**

**Comment**

Further clarification should be made to CIP-004-X Part 4.1.2 and Part 6.1.2 to address the difference between physical access to a Physical Security Perimeter that may house BCSI versus physical access to a physical piece of hardware that houses BCSI. Where does the physical piece of hardware that houses BCSI need to be stored?

Likes 0

Dislikes 0

**Response**

**Masunch Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy**

**Answer**

No

**Document Name**

**Comment**

Duke Energy agrees the proposed changes enabling entities to use third-party solutions (e.g., cloud services) for BCSI, in CIP-004-X, Requirement R6 Part 6.1, the SDT made a distinction between “electronic access to electronic BCSI” versus “physical access to physical BCSI”.

Duke Energy does not agree with, and recommends removing, “and the justification of business need for the provisioned access” as a measure in CIP-004 R6.1. Managers must be able to authorize access to a large number of employees where they would likely cut and paste a blanket justification for each person or group. All that should be required is documented authorization and removal along with the record of authorized individuals. The act of authorization should be considered sufficient that a business need for access exists. There is no risk reduction in documenting this justification, but there is significant overhead in adding such functionality to existing authorization tools.

Likes 0

Dislikes 0

### Response

**Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable**

**Answer**

Yes

**Document Name**

**Comment**

EI supports the distinctions made between “electronic access to electronic BCSI” and “physical access to physical BCSI”.

Likes 0

Dislikes 0

### Response

**Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6**

**Answer**

Yes

**Document Name**

**Comment**

“Physical BCSI” is not a defined term.

Likes 0

Dislikes 0

### Response

**Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott**

**Answer**

Yes

<b>Document Name</b>	
<b>Comment</b>	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Larry Heckert - Alliant Energy Corporation Services, Inc. - 4</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Alliant Energy supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Constantin Chitescu - Ontario Power Generation Inc. - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
OPG supports NPCC Regional Standards Committee's comments, and has the following additional comments: For 6.2 and 6.3, OPG suggest to specify that the requirement is applicable to both physical and electronic provisioned access to BCSI similar to 6.1.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	

**Comment**

Energy supports and endorses the comments filed by the Edison Electric Institute.

Likes 0

Dislikes 0

**Response**

**Gail Golden - Entergy - Entergy Services, Inc. - 5**

**Answer** Yes

**Document Name**

**Comment**

***Entergy does not oppose distinguishing electronic BCSI from physical BCSI; however, the change raises the question of how entities are to comply with 6.1.2. If someone prints out the ESP drawings on paper, must they then provide evidence of who has access to their office and how it was provisioned? Are we just going to expect that no hard copies of BCSI are created, or if so, they are only stored in a secure physical location with access controls?***

***Specifying both electronic and/or physical access to BCSI will also mirror treatment of classified information – i.e. different protection strategies apply depending on the medium. It might be cleaner to just differentiate between electronic access and physical access. If you have physical access to a Cyber Asset, you still need to somehow get access to the electronic information stored on the physical asset - electronic info protection strategies apply. If the physical asset is paper (or maybe removable media) then you may rely more heavily on physical protection strategies.***

Likes 0

Dislikes 0

**Response**

**Thomas Standifur - Austin Energy - 1,3,4,5,6**

**Answer** Yes

**Document Name** [TPWR\\_2019-02\\_Unofficial\\_Comment\\_Form\\_2021-05-10.docx20210504-17090-hsevrj.docx](#)

**Comment**

In support of Tacoma Powers' comments. Attached.

Likes 0

Dislikes 0

**Response**

**Leonard Kula - Independent Electricity System Operator - 2**

**Answer** Yes

**Document Name**

**Comment**

N/A.

Likes 0

Dislikes 0

**Response**

**Becky Webb - Exelon - 6**

**Answer** Yes

**Document Name**

**Comment**

Exelon has elected to align with EEI in response to this question.

Likes 0

Dislikes 0

**Response**

**Cynthia Lee - Exelon - 5**

**Answer** Yes

**Document Name**

**Comment**

Exelon has elected to align with EEI in response to this question.

Likes 0

Dislikes 0

**Response**

**Kinte Whitehead - Exelon - 3**

**Answer** Yes

<b>Document Name</b>	
<b>Comment</b>	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>John Galloway - ISO New England, Inc. - 2 - NPCC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
ISO New England supports this change.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Daniel Gacek - Exelon - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	

**Comment**

Southern supports the distinction between “electronic access to electronic BCSI” and “physical access to physical BCSI.”

Likes 0

Dislikes 0

**Response****David Hathaway - WEC Energy Group, Inc. - 6**

**Answer**

Yes

**Document Name**

**Comment**

Support comments made by EEI.

Likes 0

Dislikes 0

**Response****Thomas Breene - WEC Energy Group, Inc. - 3**

**Answer**

Yes

**Document Name**

**Comment**

We support EEI comments.

Likes 0

Dislikes 0

**Response**

**Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments**

**Answer**

Yes

**Document Name**

**Comment**

PG&E agrees with the modifications and clarifications.

Likes 0

Dislikes 0

**Response**

**Dan Bamber - ATCO Electric - 1**

**Answer**

Yes

**Document Name**

**Comment**

By this change, can it be clarified that an entity's IT service provider server rooms (where electronic BCSI is hosted) does not fall under physical BCSI.

Likes 0

Dislikes 0

**Response**

**Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE**

**Answer**

Yes

**Document Name**

**Comment**

OKGE supports comments provided by EEI.

Likes 0

Dislikes 0

**Response**

**Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman**

**Answer**

Yes

**Document Name**

**Comment**

MPC appreciates this distinction to enable the use of cloud service providers for entities that wish to use them and eliminate the interpretation that every possible encounter with BCSI cannot be access controlled in the way required by CIP-004, but would still be protected in another way under the entity's Information Protection Plan per CIP-011.

Likes 0

Dislikes 0

**Response**

**Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Kevin Salsbury - Berkshire Hathaway - NV Energy - 5**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Rachel Coyne - Texas Reliability Entity, Inc. - 10**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Joshua Andersen - Salt River Project - 1,3,5,6 - WECC**

**Answer** Yes

**Document Name**

<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	
<b>Response</b>	
<b>David Jendras - Ameren - Ameren Services - 3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Clarice Zellmer - WEC Energy Group, Inc. - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	

**Response**

**Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Anthony Jablonski - ReliabilityFirst - 10**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response****Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6****Answer**

Yes

**Document Name****Comment**

Likes 0

Dislikes 0

**Response****William Steiner - Midwest Reliability Organization - 10****Answer**

Yes

**Document Name****Comment**

Likes 0

Dislikes 0

**Response****Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter****Answer**

Yes

**Document Name****Comment**

Likes 0

Dislikes 0

**Response**

**Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**LaTroy Brumfield - American Transmission Company, LLC - 1**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Donna Wood - Tri-State G and T Association, Inc. - 1**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

5. The SDT considered industry comments about defining the word “access”. “Access” is broadly used across both the CIP and Operations & Planning Standards (e.g., open access) and carries different meanings in different contexts. Therefore, the SDT chose not to define “access” in the NERC Glossary of Terms. Instead, the SDT used the adjective “provisioned” to add context, thereby scoping CIP-004-X, Requirement R6. Do you agree the adjective “provisioned” in conjunction with the “Note” clarifies what “provisioned access” is? If not, please provide the basis for your disagreement and an alternate proposal.

**Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1**

**Answer** No

**Document Name**

**Comment**

CIP-004-X R2, R3, and R4 discusses authorized access. A user is to be authorized prior to being provisioned. If the CIP-004-X R6 requirements focus on provisioned users there is a gap of users who may be authorized and not yet provisioned. The SDT should chose to define authorized access in place of or in conjunction with provisioned access.

Likes 0

Dislikes 0

**Response**

**Marty Hostler - Northern California Power Agency - 3,4,5,6**

**Answer** No

**Document Name**

**Comment**

NO. NERC Terms need a definition which is to be used for both CIP and O&P standards. Else Registered Entities will be subject to Regional Entity auditor interpretations not vetted by industry.

Likes 1 Northern California Power Agency, 6, Sismaet Dennis

Dislikes 0

**Response**

**Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones**

**Answer** No

**Document Name**

**Comment**

1. Based on WAPA’s disagreement of the term “provisioned access” and given that the SDT has defined “access to BCSI” in R6, the term “provisioned access” should be removed due to the creation of an unintended security loophole (See our comments in Q1).
2. Access, which occurs in CIP standards language, whether it is electronic and/or logical access, physical access, unescorted physical access, remote access, or interactive remote access is clearly understood, has been widely adopted by industry and regulators, and has been subject to hundreds of audits across all regions for the past 14 years. Entities have developed internal documentation, configured systems, implemented controls tasks and standardized programs on these terms. The adjective “provisioned” adds further terms, requires changes and is of little value regarding the actions required of entities and the output deliverables or evidence.

**Recommendation:**

3. Revise the language to focus on access to BCSI and the auditable methods to protect BCSI at 3rd party off-prem (cloud) locations.

Likes 0

Dislikes 0

**Response**

**Dennis Sismaet - Northern California Power Agency - 6**

**Answer**

No

**Document Name**

**Comment**

Please reference Marty Hostler's comments. Thanks.

Likes 0

Dislikes 0

**Response**

**JT Kuehne - AEP - 6**

**Answer**

No

**Document Name**

**Comment**

The currently effective Requirement Part 4.1.3 of CIP-004-6 reads, “Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.” AEP suggests to use similar language from Part 4.1.3 as suggested in our response to Question #4 above. AEP recommends 6.1 use similar language to 4.1, i.e., “*Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: Access to designated storage locations, whether physical or electronic, for BES Cyber System Information*”

Likes 0

Dislikes 0

**Response**

**Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name** Dominion

**Answer** No

**Document Name**

**Comment**

Dominion Energy is concerned the the SDT is attempting to define the term "provisioned access" in a footnote. Leaving a term open to interpretation across Standards is concerning and if a term is being used inconsistently it should be defined in the Glossary of Terms rather than through a footnte for a Standard.

Likes 0

Dislikes 0

**Response**

**Bruce Reimer - Manitoba Hydro - 1**

**Answer** No

**Document Name**

**Comment**

Given that SDT has defined the "access to BCSI" in R6, the provisioned access needs to be removed since it has a unintended security loophole (See our comments in Q1).

Likes 0

Dislikes 0

**Response**

**Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name** Tacoma Power

**Answer** No

**Document Name**

**Comment**

Providing the definition of "provisioned access" within the Standard via the Note: within CIP-004 R6 Part 6.1 does not provide sufficient clarity to Industry. Tacoma Power suggests that it would be beneficial to create a NERC Glossary defined term for "Provisioned Access."

Likes	1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes	0	
<b>Response</b>		
<b>Joshua Andersen - Salt River Project - 1,3,5,6 - WECC</b>		
<b>Answer</b>	No	
<b>Document Name</b>		
<b>Comment</b>		
<p>If “provisioned” is needed, then what is non-provisioned access? SRP does don’t think “provisioned” is necessary, but adding it does not cause much concern. Access might need to be a defined term rather than using notes even if broken down between O&amp;P and CIP.</p>		
Likes	0	
Dislikes	0	
<b>Response</b>		
<b>Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations</b>		
<b>Answer</b>	No	
<b>Document Name</b>		
<b>Comment</b>		
<p>While we agree with the SDT usage of “provisioned” and the use of the “Note” to help clarify access, the “Note” does not reduce the audit risk to an Entity. The “Note” is purely there for explanation and is not a NERC accepted definition nor does it have to be accepted by an auditor. The fact this has to be explained or even noted shows the ongoing existing problem with the way “access” is used in the CIP standards.</p> <p>If a “Note” for “provisioned access” is needed to help scope “access”, then EVERY requirement with “access” in the CIP standards should have a “Note”. Defining “access” is not part of this SAR thus any modifications to “access” is out of the scope of the SAR and not a part of this change.</p> <p>Further the fact that the “Note” uses “is to be considered” is not binding to the requirement. It either is considered or not considered. The way the “Note” is written, access could or could not be “considered the result of the specific actions taken to provide an individual(s) the means to access BCSI”. If there was a way to make the “Note” binding, to be acceptable, the “Note” should be specific: “Provisioned access is the result of the specific actions taken to provide an individual(s) the means to access BCSI”. Due to the first sentence of the question, it is not possible to define “access” alone, thus definitions for various types of access could be defined such as BCSI Access in this case.</p>		
Likes	0	
Dislikes	0	
<b>Response</b>		
<b>Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1</b>		

<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<p>While we agree with the SDT usage of “provisioned” and the use of the “Note” to help clarify access, the “Note” does not reduce the audit risk to an Entity. The “Note” is purely there for explanation and is not a NERC accepted definition nor does it have to be accepted by an auditor. The fact this has to be explained or even noted shows the ongoing existing problem with the way “access” is used in the CIP standards.</p> <p>If a “Note” for “provisioned access” is needed to help scope “access”, then EVERY requirement with “access” in the CIP standards should have a “Note”. Defining “access” is not part of this SAR thus any modifications to “access” is out of the scope of the SAR and not a part of this change.</p> <p>Further the fact that the “Note” uses “is to be considered” is not binding to the requirement. It either is considered or not considered. The way the “Note” is written, access could or could not be “considered the result of the specific actions taken to provide an individual(s) the means to access BCSI”. If there was a way to make the “Note” binding, to be acceptable, the “Note” should be specific: “Provisioned access is the result of the specific actions taken to provide an individual(s) the means to access BCSI”. Due to the first sentence of the question, it is not possible to define “access” alone, thus definitions for various types of access could be defined such as BCSI Access in this case.</p> <p>AEPC has signed on to ACES comments.</p>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Thomas Standifur - Austin Energy - 1,3,4,5,6</b>	
<b>Answer</b>	No
<b>Document Name</b>	<a href="#">TPWR_2019-02_Unofficial_Comment_Form_2021-05-10.docx20210504-17090-hsevrj.docx</a>
<b>Comment</b>	
<p>In support of Tacoma Powers' comments. Attached.</p>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Gladys DeLaO - CPS Energy - 1,3,5</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	

CPS Energy suggests creating a NERC Glossary defined term for “Provisioned Access” instead of adding the Note: within CIP-004 R6 Part 6.1. Additionally, “obtain and use” should be included in the definition.

Likes 0

Dislikes 0

### Response

**Michael Brytowski - Great River Energy - 1,3,5,6**

**Answer**

No

**Document Name**

### Comment

a. Given that the SDT has defined “access to BCSI” in R6, and the term “provisioned access” should be removed due to the creation of an unintended security loophole (See our comments in Q1).

b. Access, which occurs in CIP standards language, whether it is electronic and/or logical access, physical access, unescorted physical access, remote access, or interactive remote access is clearly understood, has been widely adopted by industry and regulators, and has been subject to hundreds of audits across all regions for the past 14 years. Entities have developed internal documentation, configured systems, implemented controls tasks and standardized programs on these terms. The adjective “provisioned” adds further terms, requires changes and is of little value regarding the actions required of entities and the output deliverables or evidence.

Recommendation:

1. Revise the language to focus on access to BCSI and the auditable methods to protect BCSI at 3rd party off-prem (cloud) locations

Likes 0

Dislikes 0

### Response

**Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh**

**Answer**

No

**Document Name**

### Comment

N&ST notes that “provisioned” is not an adjective. Beyond that, “access” has already been given a contextual definition: “Obtain and use.” N&ST suggests the SDT maintain consistency with existing CIP-004 language and continue to require that Responsible Entities authorize access to BCSI and/or BCSI storage locations.

Likes 0

Dislikes 0

<b>Response</b>	
<b>Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Duke Energy agrees the adjective “provisioned” in conjunction with the “Note” clarifies what “provisioned access” is.	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
MPC supports not defining “access” as a NERC glossary term, as this could be difficult and have unintended consequences for other standards. MPC agrees that the use of “provisioned” and the note adds enough context to clarify what kind of access the requirements are about.	
Likes	0
Dislikes	0
<b>Response</b>	
<b>William Steiner - Midwest Reliability Organization - 10</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Provisioned access’ in Part 6.3 doesn’t necessarily trigger the removal of accesses granted maliciously or inadvertently, and accepts a security and reliability risk that is mitigated in today’s language. The use of provisioned access in Part 6.1 (authorize) and 6.2 (verify) is fine. Consider “... ability to access BCSI...” instead of “...ability to use provisioned access...” for Part 6.3 only	
Likes	0
Dislikes	0

**Response**

**Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE**

**Answer** Yes

**Document Name**

**Comment**

OKGE supports comments provided by EEI.

Likes 0

Dislikes 0

**Response**

**Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments**

**Answer** Yes

**Document Name**

**Comment**

PG&E agrees with the adjective “provisioned” and as noted in the comment for Question 1, will define what “provisioned” means to PG&E and following the definition in our implementation of the modifications.

Likes 0

Dislikes 0

**Response**

**Thomas Breene - WEC Energy Group, Inc. - 3**

**Answer** Yes

**Document Name**

**Comment**

We support EEI comments.

Likes 0

Dislikes 0

**Response**

**David Hathaway - WEC Energy Group, Inc. - 6**

**Answer** Yes

**Document Name**

**Comment**

Support comments made by EEI.

Likes 0

Dislikes 0

**Response**

**Clarice Zellmer - WEC Energy Group, Inc. - 5**

**Answer** Yes

**Document Name**

**Comment**

Agree with the use of term provisioned. Would like the SDT to incorporate EEI comments as a non-substantive change during the final EEI review.

Likes 0

Dislikes 0

**Response**

**Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company**

**Answer** Yes

**Document Name**

**Comment**

Southern agrees with the defining adjective of “provisioned” as the actions that may be taken to provide access to both electronic and physical BCSI. The “Note” further clarifies what possible specific actions may be considered as provisioned.

Likes 0

Dislikes 0

**Response**

**John Galloway - ISO New England, Inc. - 2 - NPCC**

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
ISO New England supports the clarification in the "Note".	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Kinte Whitehead - Exelon - 3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Cynthia Lee - Exelon - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Becky Webb - Exelon - 6</b>	
<b>Answer</b>	Yes

<b>Document Name</b>	
<b>Comment</b>	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Suggest reiterating the "Obtain and use" qualifier in the Main R6 requirement. This well better explain what "Access" really means.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Leonard Kula - Independent Electricity System Operator - 2</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
We agree that the Note clarifies provisioned access.	
We have concerns – 1) as written the reference to Part 4.1 could result in double jeopardy; 2) request clarification on how granting access in Part 4.1 could provide authorization to BCSI required in Part 6.1	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee</b>	
<b>Answer</b>	Yes

<b>Document Name</b>	
<b>Comment</b>	
We agree that the Note clarifies provisioned access.	
We have concerns – 1) as written the reference to Part 4.1 could result in double jeopardy; 2) request clarification on how granting access in Part 4.1 could provide authorization to BCSI required in Part 6.1	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Considering the R6.1 'Note,' the SDT should further clarify "provisioned access" in the IG/Technical Rationale and specifically address the "underlay" (CSP environment) from the "overlay" (SaaS, IaaS, PaaS) where "provisioned access" to BCSI is given.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Evergy supports and endorses the comments filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Benjamin Winslett - Georgia System Operations Corporation - 4</b>	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
<p>From a technical standpoint, the addition of 'provisioned' provides clear delineation regarding the definition of 'access' in this context. Please reference the above comments in questions 1 and 2 regarding inclusion of clarifying language and guidance provided in the Technical Rationale within the standard. Additionally, it is recommended that the Note regarding provisioned access be moved to the main requirement in R6 where the term "provisioned access" is first used. This will also provide clarification that the note applies to all uses of the term within the requirement and not just part 6.1.</p>	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
<b>Response</b>	
<b>Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
None.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Constantin Chitescu - Ontario Power Generation Inc. - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
<p>OPG supports NPCC Regional Standards Committee's comments, and has the following additional comments:</p> <p>Please provide additional clarification why the use of term "provisioned" is limited to access to BCSI and not also in Requirement 4 and 5.</p>	
Likes 0	
Dislikes 0	
<b>Response</b>	

**Larry Heckert - Alliant Energy Corporation Services, Inc. - 4**

**Answer** Yes

**Document Name**

**Comment**

Alliant Energy supports comments submitted by EEI.

Likes 0

Dislikes 0

**Response**

**Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)**

**Answer** Yes

**Document Name**

**Comment**

The IRC SRC has no concerns about adding “provisioned” to provide context, however, we are unsure if this helps clarify what constitutes access. Additional attempts to clarify “access” by the SDT may not be necessary. Individual entities have been successful in defining “access” for themselves and their programs whereby Attachment C and prior audit records can continue to support this approach.

Likes 0

Dislikes 0

**Response**

**Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott**

**Answer** Yes

**Document Name**

**Comment**

ITC supports the response submitted by EEI

Likes 0

Dislikes 0

**Response**

**Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC**

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Black Hills agrees with the decision, it should be evident that access is simply the ability to obtain and use, any further specifications beyond that should be an entity decision.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
EEI supports not defining "Access" and agrees that providing a NERC glossary definition could have unintended consequences. EEI supports the decision to define "provisioned access" in the context of CIP-004 to be sufficient for the purposes of this standard but also recommends that this definition be elevated to the parent Requirement R6 given that "provision access" is used throughout this requirement. (See EEI comments to Question 1)	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Donna Wood - Tri-State G and T Association, Inc. - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority</b>	

Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>LaTroy Brumfield - American Transmission Company, LLC - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	

Dislikes 0

**Response**

**Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name** Southwest Power Pool Standards Review Group (SSRG)

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name** FE Voter

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Anthony Jablonski - ReliabilityFirst - 10**

**Answer** Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Dan Bamber - ATCO Electric - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	

**Response**

**Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**David Jendras - Ameren - Ameren Services - 3**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Gail Golden - Entergy - Entergy Services, Inc. - 5**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response****Rachel Coyne - Texas Reliability Entity, Inc. - 10****Answer**

Yes

**Document Name****Comment**

Likes 0

Dislikes 0

**Response****Kevin Salsbury - Berkshire Hathaway - NV Energy - 5****Answer**

Yes

**Document Name****Comment**

Likes 0

Dislikes 0

**Response****Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6****Answer**

Yes

**Document Name****Comment**

Likes 0

Dislikes 0

**Response**

Daniel Gacek - Exelon - 1

Answer

Document Name

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0

Dislikes 0

Response

6. In response to industry concerns regarding double jeopardy or confusion with CIP-013, the SDT removed CIP-011-X, Requirement R1 Parts 1.3 and 1.4, in favor of simplifying CIP-011-X, Requirement R1 Part 1.1, and adjusting Part 1.2 to broaden the focus around the implementation of protective methods and secure handling methods to mitigate risks of compromising confidentiality. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer No

Document Name

Comment

These proposed changes have not met the requirement of the SAR to prevent unauthorized access.

CIP-011 R1 Part 1.2, should be in alignment with CIP-004 R6 Part 6.1.

While detailed instructions are addressed in, "Measures" instead of in the "requirements." Comparing with the previous draft; this version is less burdensome, and covers broader situations, and, it reduces the repeated way to present methods used in different states of transit, storage, and use. However, in 'Part 1.2 to broaden the focus on protecting and securely handling BCSI....' in this current form it is contradictory with, 'methods to protect' in the Rationale, as their objectives are different.

Recommendation:

We suggest adding "prevent unauthorized access to BCSI" to R1 Part 1.2 so that it is in alignment with CIP-004 R6.1:

"Method(s) to protect and securely handle BCSI Information to prevent unauthorized access to BCSI, including storage, transit, and use."

See the question to 'broaden' the focus of the language, and then the Technical Rationale says to be 'explicit'...this seems to be contradictory – this needs further investigation. See the new language in 1.2 as compared to the previous 1.3 & 1.4. This could result in a burden to industry here.

Likes 0

Dislikes 0

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer No

Document Name

Comment

N&ST agrees with the SDT's decision to drop proposed Requirement R1 Parts 1.3 and 1.4. However, we disagree with the proposed changes to Parts 1.1 and 1.2, as we believe the existing language adequately defines the required elements of an Information Protection Program.

Likes 0

Dislikes 0

Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
<p>While detailed instructions are addressed in, “Measures” instead of in the “requirements.” Comparing with the previous draft; this version is less burdensome, and covers broader situations, and, it reduces the repeated way to present methods used in different states of transit, storage, and use. However, in ‘Part 1.2 to broaden the focus on protecting and securely handling BCSI....’ in this current form it is contradictory with, ‘methods to protect’ in the Rationale, as their objectives are different.</p> <p>NVE suggests adding “prevent unauthorized access to BCSI” to R1 Part 1.2 so that it is in alignment with CIP-004 R6.1:</p> <p>“Method(s) to protect and securely handle BCSI Information to prevent unauthorized access to BCSI, including storage, transit, and use.”</p> <p>See the question to ‘broaden’ the focus of the language, and then the Technical Rationale says to be ‘explicit’...this seems to be contradictory – this needs further investigation. See the new language in 1.2 as compared to the previous 1.3 &amp; 1.4. This could result in a burden to industry here.</p>	
Likes	0
Dislikes	0
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
<p>Texas RE is concerned that the proposed changes remove the concept of integrity, which is as equally important as the concept of confidentiality. The current approved language in Requirement Part 1.2 specifically supports the concept of integrity through the phrase “<i>storage, transit, and use.</i>” Texas RE asserts that such comprehensive language regarding BCSI storage, transit, and use – that is ensuring confidentiality and integrity – should continue to be included. Texas RE recommends adding “and integrity” after confidentiality in Requirement Part 1.2.</p> <p>Additionally, Texas RE recommends the removal of “[i]mplementation of administrative methods” as an example of evidence for off-premise BCSI. If a Registered Entity intends to make use of third-party services for storing BCSI the Registered Entity is still responsible for ensuring the safety of the BCSI. A risk assessment or business agreement with the third-party vendor does not provide sufficient risk mitigation should the third-party vendor be compromised.</p>	

Lastly, as mentioned in response to Question #2, Texas RE recommends adding bright line criteria for determining usability of BCSI to CIP-011 Requirement Part 1.2. Texas RE recommends the following language:

1.2.1 - Method(s) to limit the ability of unauthorized individuals from obtaining or using BCSI. 1.2.2 - Method(s) to limit the ability of unauthorized individuals from modifying BCSI without being detected.

For those methods that use encryption, utilize an encryption key strength of at least 128 bits, in accordance with NIST.

For those methods that use hashing, utilize a hash function with an output size of at least 256 bits, in accordance with NIST.

Likes 0

Dislikes 0

### Response

#### Benjamin Winslett - Georgia System Operations Corporation - 4

Answer

No

Document Name

Comment

The proposed simplification is useful with the exception of the verbiage added to Requirement R1.2. Specifically, the term to mitigate the risk of compromising confidentiality is overly broad and ambiguous and could result in subjective interpretation during audits. The technical rational states that this change was made to "reduce confusion" but instead it has only added ambiguity. The existing language does not hinder the objectives of this SDT in any manner. Keeping this language consistent with the approved version of the standard will prevent unnecessary modification of existing CIP-011 programs, especially for those entities who have no desire to use cloud-hosted solutions.

As such, it is recommended that the language to R1.2 remain as follows:

Method(s) to protect and securely handle BCSI, including storage, transit, and use.

Likes 1

Georgia Transmission Corporation, 1, Davis Greg

Dislikes 0

### Response

#### Thomas Standifur - Austin Energy - 1,3,4,5,6

Answer

No

Document Name

[TPWR\\_2019-02\\_Unofficial\\_Comment\\_Form\\_2021-05-10.docx](#)[20210504-17090-hsevrj.docx](#)

Comment

In support of Tacoma Powers' comments. Attached.

Likes 0

Dislikes 0

**Response**

**Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP**

**Answer** No

**Document Name**

**Comment**

Integrity is an important security objective for 'Real-time Assessment and Real-time monitoring data' and is address in CIP-012. However, this should not negate the need to ensure the integrity of BCSI remains a security objective as well as confidentiality.

Likes 0

Dislikes 0

**Response**

**Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3**

**Answer** No

**Document Name**

**Comment**

We agree with comments from Duke Energy.

Likes 0

Dislikes 0

**Response**

**Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power**

**Answer** No

**Document Name**

**Comment**

Tacoma Power supports the inclusion of method(s) as opposed to procedure(s); however, the inclusion of the objective of "mitigate the risk of compromising confidentiality" does not follow the current language provided in CIP-012 on order to maintain Standards consistency.

Therefore, Tacoma Power suggests the following alternative language:

“Method(s) to protect and securely handle BCSI to mitigate the risks posed by unauthorized disclosure and unauthorized modification of BCSI.”

The inclusion of unauthorized modification supports the fact that entities rely on the integrity of their BCSI in many instances, and should provide protections for data integrity where there is a risk associated with data integrity.

Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
---------	---

Dislikes 0	
------------	--

**Response**

**Bruce Reimer - Manitoba Hydro - 1**

<b>Answer</b>	No
---------------	----

<b>Document Name</b>	
----------------------	--

**Comment**

We disagree with R1 Part 1.2 changes since these changes haven't resolved the goal of SAR that is to prevent unauthorized access to BCSI while in transit, storage, and in use. CIP-011 requirements should be in alignment with CIP-004 R6 Part 6.1 to ensure only authorized personnel can possess BCSI. Using "mitigate the risks.." is subjective resulting in no audit consistency since the NERC entities and auditors may have different ways to interpret it.

Likes 0	
---------	--

Dislikes 0	
------------	--

**Response**

**Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1**

<b>Answer</b>	No
---------------	----

<b>Document Name</b>	
----------------------	--

**Comment**

We agree with the removal of language of "storage, security during transit, and use" from the requirement. However, we do not see the need to mention this language again in the measures and ask that this language be removed.

Likes 0	
---------	--

Dislikes 0	
------------	--

**Response**

**Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3**

<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<p>MidAmerican Energy agrees with removal of Parts 1.3 and 1.4. However, we are concerned with the lack of clarity of the language of Part 1.2. The CIP-011-X Technical Rationale states that methods to protect BCSI “becomes explicitly comprehensive.” This question refers to a “broadened” focus, but the requirement does not clearly explain the broadened focus and comprehensive expectations. We request additional information be added to Technical Rationale regarding expectations of the requirement, including the difference between version 2 and the proposed version X.</p> <p>We agree with the removal of language of “storage, security during transit, and use” from the requirement. However, we do not see the need to mention this language again in the measures and ask that this language be removed.</p>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<p>Dominion Energy is concerned with the addition of “<i>to mitigate risks of compromising confidentiality</i>”. This additional language seems to require that Registered Entities develop methodologies and processes to determine levels of risk. Furthermore, the term <i>mitigate risks</i> is very subjective and could be interpreted differently by the respective parties involved. This addition doesn’t appear to address any risks or identified gaps. Please clarify the intent of the use of the language.</p>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>JT Kuehne - AEP - 6</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<p>AEP supports the removal of Requirement R1 Parts 1.3 and 1.4, and the minor adjustment made to Requirement R1, Part 1.1.</p> <p>AEP has concerns that the adjustments made to Requirement R1, Part 1.2, made this requirement overly broad, especially considering the management of the off-premise BCSI. Specifically, AEP is concerned with the breadth and depth of L1 and L2 evidence that would be required to demonstrate compliance and mitigating risks of compromising confidentiality associated with Requirement R1, Part 1.2 with regard to off-premise</p>	

BCSI. Further, it is not clear what would constitute acceptable methodologies or procedures (self-audit, independent audits, SOC1/SOC2 reviews, etc.) for AEP to validate a third party's control environment (provided the third party cooperates with AEP's request) sufficient to demonstrate compliance and mitigating risks of compromising confidentiality associated with Requirement R1, Part 1.2 with regard to off-premise BCSI. Finally, it is not clear to what level AEP will need to document, monitor, and enforce controls implemented and administered by a third party who maintains AEP's BCSI off-premise.

AEP is also concerned with any unintended consequences from the proposed language, as it could be interpreted to mean any vendor's use of BSCI, even if it is stored on AEP's systems, and not BSCI that is stored, transmitted, or used by a 3rd party vendors on their system(s).

Likes 0

Dislikes 0

### Response

#### William Steiner - Midwest Reliability Organization - 10

Answer No

Document Name

#### Comment

In CIP-011-X, Part 1.2, the proposed draft excludes risks related to data integrity. Omission of data integrity would require supplemental Practice Guides by the ERO Enterprise to determine what cloud environment risks are related to confidentiality vs. integrity. In practicality most data access risks overlap between those two legs of the CIA triad, and will be difficult or impossible to enforce some data risk scenarios with data confidentiality alone.

Also, the mapping document 'Description and Change Justification' indicates that the focus for CIP-011-X Part 1.2 was intended to be broader, but the change appears to be narrower than existing language. One or the other must be in error, but we are not sure which.

Likes 0

Dislikes 0

### Response

#### Dennis Sismaet - Northern California Power Agency - 6

Answer No

Document Name

#### Comment

Please reference Marty Hostler's comments. Thanks.

Likes 0

Dislikes 0

### Response

**Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones**

**Answer** No

**Document Name**

**Comment**

We do not agree with R1 Part 1.2 changes since these changes haven't resolved the goal of SAR that is to prevent unauthorized access to BCSI while in transit, storage, and in use. CIP-011 requirements should be in alignment with CIP-004 R6 Part 6.1 to ensure only authorized personnel can possess BCSI.

Recommendations:

We suggest adding "prevent unauthorized access to BCSI" to R1 Part 1.2 so that it is in alignment with CIP-004 R6.1:

"Method(s) to protect and securely handle BCSI Information to prevent unauthorized access to BCSI, including storage, transit, and use."

Likes 0

Dislikes 0

**Response**

**Marty Hostler - Northern California Power Agency - 3,4,5,6**

**Answer** No

**Document Name**

**Comment**

NO. We agree with removing CIP-011XX R1 Parts 1.3 & 1.4.

We do not agree with adjusting Part 1.2.

Likes 1

Northern California Power Agency, 6, Sismaet Dennis

Dislikes 0

**Response**

**Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1**

**Answer** No

**Document Name**

**Comment**

While more clear than the previously proposed CIP-011-3, the provided measures for CIP-011-X Part 1.2 it states, implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements). Business agreements and vendor service risk assessments does lead to confusion with CIP-013.

Likes 0

Dislikes 0

### Response

**Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy**

**Answer**

No

**Document Name**

**Comment**

Duke Energy generally agrees with the proposed changes of simplifying CIP-011-X, Requirement R1 Part 1.1, and adjusting Part 1.2 to broaden the focus around the implementation of protective methods and secure handling methods to mitigate risks of compromising confidentiality.

Duke Energy has concerns with the wording of measures for R1.2. 'on-premise BCSI' and 'off-premise BCSI' are open to interperetation. Is it the intent that a third party managed BCSI repository that is implemented on 'on-premise' servers not be subject to the 'off-premise' measures? Can a risk assessment determine the actual controls, physical, technical or administrative, needed?

Duke Energy recommends that for third party (or 'off-premise') managed or hosted storage, a risk assessment for physical, technical and administrative controls be performed and mitigating controls be implemented as determined.

Likes 0

Dislikes 0

### Response

**Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable**

**Answer**

Yes

**Document Name**

**Comment**

EI agrees with removal of Parts 1.3 and 1.4. However, we suggest additional clarity of the language in Part 1.2. The CIP-011-X Technical Rationale states that methods to protect BCSI "becomes explicitly comprehensive." This question refers to a "broadened" focus, but the requirement does not clearly explain the broadened focus and comprehensive expectations. We request additional information be added to the Technical Rationale regarding the expectations of this requirement, including the difference between Draft 2 and the proposed Draft 3 version.

EI agrees with protection of BCSI itself over the physical location in which BCSI is stored. We also support the removal of the language "storage, security during transit, and use" from this requirement. However, the language within the measure should also be removed. Furthermore, EEI does not support the use of the term "in use," because this language is not necessary or auditable.

Likes 0

Dislikes 0

**Response**

**Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC**

**Answer** Yes

**Document Name**

**Comment**

This draft is much more favorable than the previous. It's more open ended and the "confidentiality" statement aligns better with the spirit of what BCSI protection programs should aim to achieve.

Likes 0

Dislikes 0

**Response**

**Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott**

**Answer** Yes

**Document Name**

**Comment**

ITC supports the response submitted by EEI

Likes 0

Dislikes 0

**Response**

**Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)**

**Answer** Yes

**Document Name**

**Comment**

The IRC SRC supports the SDT's removal of parts 1.3 and 1.4 as retaining them in CIP-011 would have added another CIP standard to the scope of supply chain requirements. We view this as a good change.

Likes 0

Dislikes 0

**Response**

**Larry Heckert - Alliant Energy Corporation Services, Inc. - 4**

**Answer**

Yes

**Document Name**

**Comment**

Alliant Energy supports comments submitted by EEI.

Likes 0

Dislikes 0

**Response**

**Constantin Chitescu - Ontario Power Generation Inc. - 5**

**Answer**

Yes

**Document Name**

**Comment**

OPG supports NPCC Regional Standards Committee's comments.

Likes 0

Dislikes 0

**Response**

**Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2**

**Answer**

Yes

**Document Name**

**Comment**

None.

Likes 0

Dislikes 0

**Response**

Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer

Answer Yes

Document Name

**Comment**

Evergy supports and endorses the comments filed by the Edison Electric Institute.

Likes 0

Dislikes 0

**Response**

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer Yes

Document Name

**Comment**

We agree with this simplification.

Likes 0

Dislikes 0

**Response**

Leonard Kula - Independent Electricity System Operator - 2

Answer Yes

Document Name

**Comment**

We agree with this simplification.

Likes 0

Dislikes 0

**Response**

Becky Webb - Exelon - 6

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Cynthia Lee - Exelon - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Kinte Whitehead - Exelon - 3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>John Galloway - ISO New England, Inc. - 2 - NPCC</b>	
<b>Answer</b>	Yes

**Document Name**

**Comment**

ISO New England agrees with this simplification.

Likes 0

Dislikes 0

**Response**

**Daniel Gacek - Exelon - 1**

**Answer**

Yes

**Document Name**

**Comment**

Exelon has elected to align with EEI in response to this question.

Likes 0

Dislikes 0

**Response**

**Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company**

**Answer**

Yes

**Document Name**

**Comment**

Southern supports the deletion of CIP-011-X Requirement R1 Parts 1.3 and 1.4 and simplifying Parts 1.1 and 1.2. The SDT has made it clear the protection of BCSI itself is what is addressed here over where the BCSI is actually stored.

Likes 0

Dislikes 0

**Response**

**David Hathaway - WEC Energy Group, Inc. - 6**

**Answer**

Yes

**Document Name**

**Comment**

Support comments made by EEI.

Likes 0

Dislikes 0

**Response**

**Thomas Breene - WEC Energy Group, Inc. - 3**

**Answer**

Yes

**Document Name**

**Comment**

We support EEI comments.

Likes 0

Dislikes 0

**Response**

**Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments**

**Answer**

Yes

**Document Name**

**Comment**

PG&E does not believe there is any double jeopardy between the proposed modifications to CIP-011-X and CIP-013.

Likes 0

Dislikes 0

**Response**

**Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE**

**Answer**

Yes

**Document Name**

**Comment**

OKGE supports comments provided by EEI.

Likes 0

Dislikes 0

**Response**

**Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman**

**Answer**

Yes

**Document Name**

**Comment**

MPC agrees with the proposed changes and believes that CIP-011 requires protection of BCSI no matter where it is located. To do this, entities must conduct assessments to understand what BCSI they have, where it can be found, how it transmits, what is done with it, and understand how confidentiality could be compromised at any of these times and locations in order to implement appropriate controls to protect it.

While MPC appreciates the reminder in the measures to consider BCSI that is located on-premises and off-premises, using these terms here may be confusing. MPC suggests including additional information in Technical Rationale or Implementation Guidance instead.

Likes 0

Dislikes 0

**Response**

**Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD**

**Answer**

Yes

**Document Name**

**Comment**

In the Measures for R1.2, change "on-premise" to "on-premises" and "off-premise" to "off-premises".

Likes 0

Dislikes 0

**Response**

**Michael Brytowski - Great River Energy - 1,3,5,6**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Gladys DeLaO - CPS Energy - 1,3,5**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Gail Golden - Entergy - Entergy Services, Inc. - 5**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1**

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0

**Response**

**Clarice Zellmer - WEC Energy Group, Inc. - 5**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Dan Bamber - ATCO Electric - 1**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Anthony Jablonski - ReliabilityFirst - 10**

**Answer**

Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	

**Response**

**LaTroy Brumfield - American Transmission Company, LLC - 1**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Donna Wood - Tri-State G and T Association, Inc. - 1**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

7. The SDT extended the implementation plan to 24-months in an attempt to align with the Project 2016-02 modifications that are on the same drafting timeline, and added an optional provision for early adoption. Do you agree this approach gives industry adequate time to implement without encumbering entities who are planning to, or are already using, third-party solutions (e.g., cloud services) for BCSI? If not, please provide the basis for your disagreement and an alternate proposal

**Dennis Sismaet - Northern California Power Agency - 6**

**Answer** No

**Document Name**

**Comment**

Please reference Marty Hostler's comments. Thanks.

Likes 0

Dislikes 0

**Response**

**Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy**

**Answer** Yes

**Document Name**

**Comment**

Duke Energy agrees with the extension of the 24-months implementation plan provided the CIP-004 R6.1 requirement to document justification of the need for authorization is eliminated.

Likes 0

Dislikes 0

**Response**

**Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman**

**Answer** Yes

**Document Name**

**Comment**

MPC agrees with this approach.

Likes 0

Dislikes 0

**Response**

**Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments**

**Answer** Yes

**Document Name**

**Comment**

PG&E agrees with the 24-month implementation plan and the ability for early adoption.

Likes 0

Dislikes 0

**Response**

**David Hathaway - WEC Energy Group, Inc. - 6**

**Answer** Yes

**Document Name**

**Comment**

Support comments made by EEI.

Likes 0

Dislikes 0

**Response**

**Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company**

**Answer** Yes

**Document Name**

**Comment**

Southern agrees with the 24-month timeline. It will allow enough time to reach implementation.

Likes 0

Dislikes 0

**Response**

**Daniel Gacek - Exelon - 1**

<b>Answer</b>	Yes
---------------	-----

<b>Document Name</b>	
----------------------	--

<b>Comment</b>
----------------

Exelon has elected to align with EEI in response to this question.

Likes 0	
---------	--

Dislikes 0	
------------	--

<b>Response</b>
-----------------

**John Galloway - ISO New England, Inc. - 2 - NPCC**

<b>Answer</b>	Yes
---------------	-----

<b>Document Name</b>	
----------------------	--

<b>Comment</b>
----------------

ISO New England agrees with aligning timelines.

Likes 0	
---------	--

Dislikes 0	
------------	--

<b>Response</b>
-----------------

**Kinte Whitehead - Exelon - 3**

<b>Answer</b>	Yes
---------------	-----

<b>Document Name</b>	
----------------------	--

<b>Comment</b>
----------------

Exelon has elected to align with EEI in response to this question.

Likes 0	
---------	--

Dislikes 0	
------------	--

<b>Response</b>
-----------------

**Cynthia Lee - Exelon - 5**

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Becky Webb - Exelon - 6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Leonard Kula - Independent Electricity System Operator - 2</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
We agree with aligning timelines.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	

**Comment**

We agree with aligning timelines.

Likes 0

Dislikes 0

**Response**

**Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer**

**Answer**

Yes

**Document Name**

**Comment**

Evergy supports and endorses the comments filed by the Edison Electric Institute.

Likes 0

Dislikes 0

**Response**

**Benjamin Winslett - Georgia System Operations Corporation - 4**

**Answer**

Yes

**Document Name**

**Comment**

Yes, 24 months is sufficient and aligning the changes with the Project 2016-02 SDT modifications will improve the efficiency and cost-effectiveness of the adjustments required to comply with these modifications.

Likes 1

Georgia Transmission Corporation, 1, Davis Greg

Dislikes 0

**Response**

**Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2**

**Answer**

Yes

**Document Name**

**Comment**

None.

Likes 0

Dislikes 0

**Response**

**Constantin Chitescu - Ontario Power Generation Inc. - 5**

**Answer**

Yes

**Document Name**

**Comment**

OPG supports NPCC Regional Standards Committee's comments.

Likes 0

Dislikes 0

**Response**

**Larry Heckert - Alliant Energy Corporation Services, Inc. - 4**

**Answer**

Yes

**Document Name**

**Comment**

Alliant Energy supports comments submitted by EEI.

Likes 0

Dislikes 0

**Response**

**Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)**

**Answer**

Yes

**Document Name**

**Comment**

The IRC SRC acknowledges the SDT for incorporating our prior suggestion for added flexibility.

Likes 0

Dislikes 0

**Response**

**Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott**

**Answer**

Yes

**Document Name**

**Comment**

ITC supports the response submitted by EEI

Likes 0

Dislikes 0

**Response**

**Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable**

**Answer**

Yes

**Document Name**

**Comment**

EEI supports the proposal to extend the implementation plan to 24-months because changes will be necessary to align processes and training with the new requirements for both entities planning to utilize cloud services as well as those not planning to do so. EEI also supports the option for early adoption.

Likes 0

Dislikes 0

**Response**

**Donna Wood - Tri-State G and T Association, Inc. - 1**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Marty Hostler - Northern California Power Agency - 3,4,5,6**

**Answer** Yes

**Document Name**

**Comment**

Likes 1 Northern California Power Agency, 6, Sismaet Dennis

Dislikes 0

**Response**

**Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**LaTroy Brumfield - American Transmission Company, LLC - 1**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**William Steiner - Midwest Reliability Organization - 10**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**JT Kuehne - AEP - 6**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Anthony Jablonski - ReliabilityFirst - 10**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Dan Bamber - ATCO Electric - 1**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Bruce Reimer - Manitoba Hydro - 1**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Clarice Zellmer - WEC Energy Group, Inc. - 5**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**David Jendras - Ameren - Ameren Services - 3**

Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	
<b>Response</b>	
<b>Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Joshua Andersen - Salt River Project - 1,3,5,6 - WECC</b>	
Answer	Yes
Document Name	
<b>Comment</b>	

Likes 0

Dislikes 0

**Response**

**Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE**

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Gail Golden - Entergy - Entergy Services, Inc. - 5</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Kevin Salsbury - Berkshire Hathaway - NV Energy - 5</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Gladys DeLaO - CPS Energy - 1,3,5</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0

**Response**

**Michael Brytowski - Great River Energy - 1,3,5,6**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC**

**Answer**

Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Thomas Standifur - Austin Energy - 1,3,4,5,6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Thomas Breene - WEC Energy Group, Inc. - 3</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
We support EEI comments.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Rachel Coyne - Texas Reliability Entity, Inc. - 10</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
Texas RE does not have comments on this question.	

Likes 0

Dislikes 0

**Response**

8. In looking at all proposed recommendations from the standard drafting team, are the proposed changes a cost-effective approach?

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer No

Document Name

Comment

Unknown fiscal impacts without a cost impact analysis and further clarifications.

PAC has strong concerns regarding the broadened and “explicitly comprehensive” expectations for CIP-011-X R1.2, which could result in significant impacts that are not cost-effective.

Standards should not be approved by until each SDT develop a detailed cost estimate.

There is no information to determine if the modifications are a cost-effective approach

Likes 0

Dislikes 0

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer No

Document Name

Comment

N&ST’s selection of “No” reflects our belief that currently proposed changes should be amended.

Likes 0

Dislikes 0

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer No

Document Name

Comment

Unknown at this time. The broadened approach to BCSI protections in CIP-011, could lead to potential high costs to an Entity.

Likes 0

Dislikes 0

**Response**

**Joshua Andersen - Salt River Project - 1,3,5,6 - WECC**

**Answer**

No

**Document Name**

**Comment**

SRP still holds to our comments from last time - the cost to implement will grow quickly with unclear requirements that lead to Responsible Entity concerns of proper interpretation. We would not say these are cost-effective at this time

Likes 0

Dislikes 0

**Response**

**Becky Webb - Exelon - 6**

**Answer**

No

**Document Name**

**Comment**

Unfortunately we wouldnt be able to properly answer this question at this time.

Likes 0

Dislikes 0

**Response**

**Kinte Whitehead - Exelon - 3**

**Answer**

No

**Document Name**

**Comment**

Unfortunately we wouldnt be able to properly answer this question at this time.

Likes 0

Dislikes 0

**Response**

**Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1**

**Answer** No

**Document Name**

**Comment**

MidAmerican Energy is concerned with broadened and “explicitly comprehensive” expectations for CIP-011-X R1.2, which could result in a costly approach.

Likes 0

Dislikes 0

**Response**

**Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments**

**Answer** No

**Document Name**

**Comment**

At this time PG&E does not have information to determine if the modifications are a cost-effective approach.

Likes 0

Dislikes 0

**Response**

**Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3**

**Answer** No

**Document Name**

**Comment**

MidAmerican Energy is concerned with broadened and “explicitly comprehensive” expectations for CIP-011-X R1.2, which could result in a costly approach.

Likes 0

Dislikes 0

**Response****Dennis Sismaet - Northern California Power Agency - 6**

**Answer**

No

**Document Name**

**Comment**

Please reference Marty Hostler's comments. Thanks.

Likes 0

Dislikes 0

**Response****Marty Hostler - Northern California Power Agency - 3,4,5,6**

**Answer**

No

**Document Name**

**Comment**

The SDT has not provided a cost estimate. Consequently, we have no idea if the proposal is cost effective.

Standards should not be approved by Industry until each Standard Drafting Team develops a detailed cost estimate (capital and maintenance).

This means including internal controls, more staff, management/board approval, budgetting, revising all Internal Compliance Documents to account for the new standard or modifications, etc. All these changes end up costing real people, our customer, they certainly would not blindly tell the STD I just want that product and don't care what the cost is.

Likes 1

Northern California Power Agency, 6, Sismaet Dennis

Dislikes 0

**Response**

**Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy**

**Answer** No

**Document Name**

**Comment**

Duke Energy recommends removing “and the justification of business need for the provisioned access” as a measure in CIP-004 R6.1. Managers must be able to authorize access to a large number of employees without need to cut and paste a blanket justification for each person or group. All that should be required is documented authorization and removal along with the record of authorized individuals. The act of authorization should be considered sufficient that a business need for access exists. There is no risk reduction in documenting this justification, but there is significant overhead in adding such functionality to existing authorization tools.

Likes 0

Dislikes 0

**Response**

**Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1**

**Answer** No

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)**

**Answer** Yes

**Document Name**

**Comment**

The proposed changes appear to be backwards compatible, allowing entities to quickly adapt current compliance programs to incorporate the changes and are a substantial improvement over the last draft.

Likes 0

Dislikes 0

**Response**

**Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2**

**Answer** Yes

**Document Name**

**Comment**

None.

Likes 0

Dislikes 0

**Response**

**Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company**

**Answer** Yes

**Document Name**

**Comment**

Southern agrees that the proposed changes are cost effective. There may be additional costs in the future for the use of different technology or applications but would be budgeted for any planned upgrades.

Likes 0

Dislikes 0

**Response**

**Thomas Breene - WEC Energy Group, Inc. - 3**

**Answer** Yes

**Document Name**

**Comment**

We think this is a cost effective way to address the issue.

Likes 0

Dislikes 0

**Response**

**Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones**

Answer	Yes
Document Name	
<b>Comment</b>	
Any changes made result in a cost to industry.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
<b>Comment</b>	
See comments in response to #9 below.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thomas Standifur - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
<b>Comment</b>	

Likes 0

Dislikes 0

**Response**

**Larry Heckert - Alliant Energy Corporation Services, Inc. - 4**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Michael Brytowski - Great River Energy - 1,3,5,6**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Gladys DeLaO - CPS Energy - 1,3,5**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Benjamin Winslett - Georgia System Operations Corporation - 4**

Answer Yes

Document Name

Comment

Likes 1

Georgia Transmission Corporation, 1, Davis Greg

Dislikes 0

Response

**Gail Golden - Entergy - Entergy Services, Inc. - 5**

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

**Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1**

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

**Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations**

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

**Response**

**Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Clarice Zellmer - WEC Energy Group, Inc. - 5**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**David Hathaway - WEC Energy Group, Inc. - 6**

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Bruce Reimer - Manitoba Hydro - 1</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Dan Bamber - ATCO Electric - 1</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0

**Response**

**Anthony Jablonski - ReliabilityFirst - 10**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**JT Kuehne - AEP - 6**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**William Steiner - Midwest Reliability Organization - 10**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter**

**Answer**

Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name</b>	Southwest Power Pool Standards Review Group (SSRG)
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>LaTroy Brumfield - American Transmission Company, LLC - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	

**Response**

**Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Donna Wood - Tri-State G and T Association, Inc. - 1**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott**

**Answer**

**Document Name**

**Comment**

No comment

Likes 0

Dislikes 0

**Response**

**Rachel Coyne - Texas Reliability Entity, Inc. - 10**

**Answer****Document Name****Comment**

Texas RE does not have comments on this question.

Likes 0

Dislikes 0

**Response**

**Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer**

**Answer****Document Name****Comment**

Evergy supports and endorses the comments filed by the Edison Electric Institute.

Likes 0

Dislikes 0

**Response**

**Leonard Kula - Independent Electricity System Operator - 2**

**Answer****Document Name****Comment**

N/A.

Likes 0

Dislikes 0

**Response**

**Cynthia Lee - Exelon - 5**

**Answer**

**Document Name**

**Comment**

Unfortunately we wouldnt be able to properly answer this question at this time.

Likes 0

Dislikes 0

**Response**

**Daniel Gacek - Exelon - 1**

**Answer**

**Document Name**

**Comment**

Unfortunately we wouldnt be able to properly answer this question at this time.

Likes 0

Dislikes 0

**Response**

**9. Please provide any additional comments for the SDT to consider, if desired.**

**Donna Wood - Tri-State G and T Association, Inc. - 1**

**Answer**

**Document Name**

**Comment**

Tri-State Generation and Transmission appreciates the time and effort given to this project and agrees with the revisions/changes.

Likes 0

Dislikes 0

**Response**

**Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy**

**Answer**

**Document Name**

**Comment**

No additional comments.

Likes 0

Dislikes 0

**Response**

**Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority**

**Answer**

**Document Name**

**Comment**

The proposed language is too ambiguous and obligates entities to protect BCSI in any form, even though beyond its control. Should BCSI be shared with NERC/FERC, the proposed standard would require registered entities to extend their access management to include the copy of that information held by NERC/FERC. Subsequent requirements in CIP-011 would require reviews of access rights associated with that copy.

The language should be re-scoped to focus on management of access to designated repositories, instead of the information itself.

Likes 0

Dislikes 0

**Response**

**Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1**

**Answer**

**Document Name**

**Comment**

The CIP-004-X and CIP-011-X proposal is more favorable than the previous CIP-004-7 and CIP-011-3 approach of moving access management of BCSI from CIP-004 and adding it to CIP-011.

Likes 0

Dislikes 0

**Response**

**Marty Hostler - Northern California Power Agency - 3,4,5,6**

**Answer**

**Document Name**

**Comment**

none.

Likes 1

Northern California Power Agency, 6, Sismaet Dennis

Dislikes 0

**Response**

**Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones**

**Answer**

**Document Name**

**Comment**

The SDT should work to simplify but clarify the standards. Years down the road auditors make interpretations and companies need to be clear what is required. Secondly the SDT should look at ISO and NIST standards for guidance. Per our comments in question 1, WAPA recommends changing “provisioned access” to “access to BCSI” for whole R6 and its parts as suggested here:

“Except our suggested changes to R6 Part 6.1, we also have the following recommendations for R6 Part 6.2 and 6.3:

- For changes to R6 Part 6.2:

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

6.2.1. have an Is authorization record;

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

- For changes to R6 Part 6.3:

For termination actions, remove the individual’s ability to 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.”

As we suggested in Q1, changing from “provisioned access to BCSI” to “access to BCSI” provides the clarity and flexibility for authorizing, verifying, and revoking access” to BCSI using various approaches including BCSI repository level or BCSI file level protection, which make the R6 backwards compatible.

Likes	0
-------	---

Dislikes	0
----------	---

<b>Response</b>
-----------------

<b>Dennis Sismaet - Northern California Power Agency - 6</b>
--

<b>Answer</b>
---------------

<b>Document Name</b>
----------------------

<b>Comment</b>
----------------

Please reference Marty Hostler's comments. Thanks.

Likes	0
-------	---

Dislikes	0
----------	---

<b>Response</b>
-----------------

<b>Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)</b>
---

<b>Answer</b>
---------------

**Document Name**

**Comment**

The SSRG wants to thank the drafting team for their time and efforts on this project.

Likes 0

Dislikes 0

**Response**

**Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter**

**Answer**

**Document Name**

**Comment**

N/A

Likes 0

Dislikes 0

**Response**

**JT Kuehne - AEP - 6**

**Answer**

**Document Name**

**Comment**

No further comments.

Likes 0

Dislikes 0

**Response**

**Anthony Jablonski - ReliabilityFirst - 10**

**Answer**

**Document Name**

**Comment**

CIP-004-X R6 and CIP-011-X R1 have different applicability. In the Draft 3 language, BCSI pertaining to medium impact BCS without ERC must be protected (CIP-011-X R1), but access to this BCSI need not be controlled (CIP-004-X R6). Without mandated access controls, the entity will be left to determine what is an effective protection to BCSI pertaining to medium impact BCS without ERC. The SDT should consider revisiting the differences in applicability between CIP-004-X R6 and CIP-011-X R1. Since this issue is beyond the scope of the 2019-02 SAR, please add this concern to the list of SAR items for the next revision of CIP-004.

The Background sections of CIP-004-x and CIP-011-X should be moved to their respective Technical Rationale documents.

CIP-004-X Implementation Guidance: 1) Implementation Guidance for R2 states that “a single training program for all individuals needing to be trained is acceptable” which is in conflict with the language in R2, “appropriate to individual roles, functions, or responsibilities.” 2) Page numbers for R6 are incorrect. 3) Appendix 1 should be moved to the Technical Rationale document as it does not fit the requirements for Implementation Guidance.

Implementation Plan: The “Early Adoption” paragraph should make it clear that all of the updated Requirements must be adopted at the same time. An entity should not be permitted to early-adopt only parts of the revised Standards.

Likes 0

Dislikes 0

### Response

**Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE**

**Answer**

**Document Name**

**Comment**

OKGE supports comments provided by EEI.

Likes 0

Dislikes 0

### Response

**Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3**

**Answer**

**Document Name**

**Comment**

MidAmerican Energy continues to have concern with the revised text of CIP-004-X R6.2. Please add a statement to the CIP-004-X Technical Rationale document: The review expected in CIP-004-X R6.2 is expected to be the same as CIP-004-6 R4.4.

While we are generally supportive of the changes to CIP-004, we are concerned about creating a new separate requirement for BCSI authorization, revocation and review. This creates the potential for non compliance of multiple requirements for a single situation, such as revocation of accesses for a termination. We ask the SDT to consider making changes that will reconcile this issue.

Likes 0

Dislikes 0

### Response

**Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments**

**Answer**

**Document Name**

**Comment**

PG&E thanks the SDT for the effort in making the modifications objective based that will allow PG&E to implement them to fit our environment.

Likes 0

Dislikes 0

### Response

**Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1**

**Answer**

**Document Name**

**Comment**

MidAmerican Energy continues to have concern with the revised text of CIP-004-X R6.2. Please add a statement to the CIP-004-X Technical Rationale document: The review expected in CIP-004-X R6.2 is expected to be the same as CIP-004-6 R4.4.

While we are generally supportive of the changes to CIP-004, we are concerned about creating a new separate requirement for BCSI authorization, revocation and review. This creates the potential for non compliance of multiple requirements for a single situation, such as revocation of accesses for a termination. We ask the SDT to consider making changes that will reconcile this issue.

Likes 0

Dislikes 0

### Response

**Thomas Breene - WEC Energy Group, Inc. - 3**

**Answer**

**Document Name**

**Comment**

We support EEI comments.

Likes 0

Dislikes 0

**Response**

**Bruce Reimer - Manitoba Hydro - 1**

**Answer**

**Document Name**

**Comment**

Resulting from our comments in Q1, we suggest changing “provisioned access” to “access to BCSI” for whole R6 and its parts.

**Recommendations:**

Except our suggested changes to R6 Part 6.1, we also have the following recommendations for R6 Part 6.2 and 6.3:

For changes to R6 Part 6.2:

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

6.2.1. have an authorization record;

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

For changes to R6 Part 6.3:

For termination actions, remove the individual’s ability to 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.

As we suggested in Q1, changing from “provisioned access to BCSI” to “access to BCSI” would provide the clarity and the flexibility for authorizing, verifying, and revoking access” to BCSI using various approaches including BCSI repository level or BCSI file level protection, which make the R6 backwards compatible.

Likes 0

Dislikes 0

**Response**

**David Hathaway - WEC Energy Group, Inc. - 6**

**Answer**

**Document Name**

**Comment**

Support comments made by EEI.

Likes 0

Dislikes 0

**Response**

**Clarice Zellmer - WEC Energy Group, Inc. - 5**

**Answer**

**Document Name**

**Comment**

Supportive of EEI comments on this project.

Likes 0

Dislikes 0

**Response**

**Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power**

**Answer**

**Document Name**

**Comment**

Tacoma Power supports the objective of the Project 2019-02 SAR, which includes providing a path to allow the use of modern third-party data storage and analysis systems. While the use of third-party data storage may be enabled to a degree with these modifications, the use of third-party analysis systems is likely not. Any managed security provider's solution would likely be considered an EACMS based on the current definition, which carries a host of CIP Requirements, not the least of which are found in CIP-004, which would preclude the use of these services in almost every case.

Tacoma Power suggests modification of the EACMS NERC Glossary definition to split off access control from access monitoring, which then would allow for requirement applicability based on risk for access control systems versus access monitoring systems.

Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	
<b>Response</b>	
<b>Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
PNM Resources appreciates the work of the SDT and the opportunity to provide feedback.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Joshua Andersen - Salt River Project - 1,3,5,6 - WECC</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
CIP-004 R6.2, in the Measures, suggest removing "Verification that provisioned access is appropriate based on need" – the need is confirmed by the authorization of access. Also, the measure should align with the requirement 6.2.2, which does not say "based on need"	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Leonard Kula - Independent Electricity System Operator - 2</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
Request clarification on Part 6.2's Measures. Will auditing / enforcement expect every item? This Measure starts with "Examples of evidence may include." Does the SDT mean this "may" is a "shall?" Recommend changing "Examples" to "Example."	

We look forward to seeing the final combined version of this update and the virtualization update.

Likes 0

Dislikes 0

**Response**

**Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee**

**Answer**

**Document Name**

**Comment**

Request clarification on Part 6.2's Measures. Will auditing/enforcement expect every item? This Measure starts with "Examples of evidence may include." Does the SDT mean this "may" is a "shall?" Recommend changing "Examples" to "Example."

We look forward to seeing the final combined version of this update and the virtualization update.

Likes 0

Dislikes 0

**Response**

**Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations**

**Answer**

**Document Name**

**Comment**

We would like to thank the SDT for allowing us to comment.

Likes 0

Dislikes 0

**Response**

**Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1**

**Answer**

**Document Name**

**Comment**

Thank you for the opportunity to comment.

Likes 0

Dislikes 0

**Response**

**Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer**

**Answer**

**Document Name**

**Comment**

Evergy supports and endorses the comments filed by the Edison Electric Institute.

Likes 0

Dislikes 0

**Response**

**Benjamin Winslett - Georgia System Operations Corporation - 4**

**Answer**

**Document Name**

**Comment**

These changes are viewed as an overall improvement to the requirements around BCSI in CIP-004 and CIP-011. However, it would be more effective if these requirements were integrated into the existing framework of CIP-004 R4 and R5 rather than creating a new requirement R6. As it is now proposed, entities will need to recognize that authorizations are now covered in R4 and R6, periodic access reviews now exist in R4 and R6, and revocations are required in both R5 and R6. While the requirements are outlined reasonably, this separation creates a new burden on readability of the standards and training new staff regarding compliance expectations.

Likes 1

Georgia Transmission Corporation, 1, Davis Greg

Dislikes 0

**Response**

**Rachel Coyne - Texas Reliability Entity, Inc. - 10**

**Answer**

**Document Name****Comment**

Texas RE is concerned by now explicitly including the concept of confidentiality in CIP-011, Part 1.2, the SDT has inadvertently removed the concept of integrity from the scope of the proposed CIP-011. As noted in Texas RE's response to Question 6, the current approved language in CIP-011 that states "*storage, transit, and use*" in Part 1.2 supports the concept of integrity. Texas RE recommends adding "and integrity" after confidentiality in Requirement Part 1.2.

Texas RE also recommends including a bright line criteria for determining usability of BCSI to CIP-011 Requirement Part 1.2 should be established to ensure consistent application of the standard.

Likes 0

Dislikes 0

**Response****Gladys DeLaO - CPS Energy - 1,3,5****Answer****Document Name****Comment**

CPS Energy does not have any additional comments at this time.

Likes 0

Dislikes 0

**Response****Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2****Answer****Document Name****Comment**

ERCOT hereby incorporates the comments filed by the ISO/RTO Council Standards Review Committee. In addition the ISO/RTO Council comments, ERCOT offers the following additional comments. First, with respect to Reliability Standard CIP-004-x, Requirement 6, Parts 6.1 and 6.2, the concept of roles should be allowed to be consistent with Requirement R4. This could be addressed in the requirement language or accompanying measure. If this is not permitted, ERCOT would appreciate an explanation explain why in the consideration of comments. Second, ERCOT believes the SDT should address the ability to use third-party audit reports in verifying the controls for third parties. Similarly, ERCOT would appreciate an explanation whether this is allowed or not, and why.

Likes 0

Dislikes 0

**Response**

**Constantin Chitescu - Ontario Power Generation Inc. - 5**

**Answer**

**Document Name**

**Comment**

OPG supports NPCC Regional Standards Committee's comments, and has the following additional comments:

CIP 004-X 4.1 requires entity to have a "process"; where 6.1 requires the entity to authorize but a "process" is not required. Both requirements seem to have similar intent with 4.1 applying to the Applicable System and 6.1 applying to BSCI. Please provide clarification whether the discrepancy is intentional.

Likes 0

Dislikes 0

**Response**

**Michael Brytowski - Great River Energy - 1,3,5,6**

**Answer**

**Document Name**

**Comment**

1. Resulting from our comments in Q1, we suggest changing "provisioned access" to "access to BCSI" for whole R6 and its parts. Except our suggested changes to R6 Part 6.1, we also have the following recommendations for R6 Part 6.2 and 6.3:

&bull; For changes to R6 Part 6.2:

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

6.2.1. have an Is authorization record;

6.2.2. Is still need the access to BCSI to perform their current work functions, appropriate based on need, as determined by the Responsible Entity.

&bull; For changes to R6 Part 6.3:

For termination actions, remove the individual's ability to 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.

We believe "access to BCSI" provides the flexibility for authorizing, verifying, and revoking access" to BCSI using various approaches including BCSI repositories and BCSI files, which make the R6 backwards compatible.

2. The SDT may consider cleaning up the language to potentially the following language:

R6. Each Responsible Entity shall implement an access management program(s) to authorize, verify, and revoke access to 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 CIP004-X Table R6 – Access Management for BES Cyber System Information.

[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]

Revised Language Recommendations

6.1 Prior to authorization (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. Electronic access to electronic BCSI; and

6.1.2. Physical access to physical BCSI. Note: 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)

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

6.2.1. Have a current authorization record; and

6.2.2. A justification for authorization to perform their current work functions, as determined by the Responsible Entity.

Likes 0

Dislikes 0

**Response**

**Larry Heckert - Alliant Energy Corporation Services, Inc. - 4**

**Answer**

**Document Name**

**Comment**

Alliant Energy supports comments submitted by EEI.

Likes 0

Dislikes 0

**Response**

**Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name** ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)

**Answer**

**Document Name**

[2019-02\\_Unofficial\\_Comment\\_Form\\_BCSI Access Management\\_IRC SRC\\_05-10-21\\_FINAL.docx](#)

**Comment**

**CIP-011-X, Part 1.2, Measures:** The IRC SRC recommends the SDT clarify that encrypted information, also known as cipher text, is not BCSI.

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, <delete cipher,> electronic key management); or

Note: MISO abstains from the response to item 9.

Likes 0

Dislikes 0

### Response

**Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott**

**Answer**

**Document Name**

**Comment**

ITC supports the response submitted by EEI

Likes 0

Dislikes 0

### Response

**Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh**

**Answer**

**Document Name**

**Comment**

N&ST has two additional comments, and associated recommendations, to respectfully offer.

The first comment is that in our opinion, the proposed changes do not address one of the project's stated goals, which is "...to clarify the protections expected when utilizing third-party solutions (e.g., cloud services)." N&ST is aware of the SDT's desire to avoid writing overly prescriptive requirements, such as was done in the first set of proposed revisions to CIP-011, but we nonetheless believe the issue of who is creating, and has the potential ability to use, authentication credentials such as encryption keys must be addressed in the Standards in one or more Requirements (vs. in "Measures" or guidance documents). We are aware of one Responsible Entity that was found by a Regional Entity audit team to be out of compliance with CIP-004 for storing BCSI in the cloud and relying on the cloud service provider's default encryption. Simply dropping "storage locations" from CIP-004 would not, by itself, have helped the Responsible Entity avoid this problem. N&ST therefore recommends the following or similar language be added to either CIP-004 or CIP-011:

“The Responsible Entity shall ensure that all individuals, including those affiliated with third parties such as vendors and cloud service providers, who possess the means to obtain and use BCSI that is protected by one or more electronic and/or physical access controls (login credentials, unlock passwords, encryption keys, cardkeys, brass keys, etc.) have been authorized in accordance with CIP-004 requirements.”

N&ST’s second comment is that we are concerned there is insufficient clarity with regards to what distinguishes “provisioning” from “sharing.” During the recent SDT webinar, a member of the SDT gave listeners a good example: (paraphrasing) Person A, who has been provisioned access to a file cabinet and has a key, opens it and gives a BCSI document to Person B, who has not been authorized for access to the file cabinet and cannot open it. Person A has shared BCSI with Person B. The SDT has already created a contextual definition of “access to BCSI.” N&ST recommends that a similar contextual definition of “sharing” be added to either CIP-004 or CIP-011, working off the example the SDT itself created.

Likes 0

Dislikes 0

### Response

**Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6**

**Answer**

**Document Name**

**Comment**

Recommend creating a NERC Glossary defined term for “Provisioned Access.”

“Physical BCSI” is not a defined term.

“Storage Locations” is no longer explicitly stated.

The language should be re-scoped to focus on management of access to designated repositories

We appreciate all the time and effort given to this project to develop these revisions/changes.

However, if you are approving a new set of Standards, we recommend that the Technical Guidance is also published at the same time. The excessive delay between these publications, is causing industry confusion.

The VSL – this is excessively severe (Proposed VSLs are based on a single violation and not cumulative violations.)

Recommend:

Use the same language as previously in R4:

**R4: Operations Planning and Same Day Operations – VRF Medium** The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)

Authorize happens *prior* to provisioning access R6.R1 – See Note: The SDT is relying HEAVILY on the CMEP guide for definition parameters, and not the STD language.

Clarify BOTH CIP-004 & CIP-011 requirements relating to managing access and protecting BCSI.

Likes 0

Dislikes 0

**Response**

**Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable**

**Answer**

**Document Name**

**Comment**

EEl is concerned with having two separate requirements within CIP-004-X that address access removal. (See Requirement R5 (BCS) and R6 (BCSI) While we understand the intent and reasons for this change, often access is provided to individuals for both BCS and BCSI and any failure in the termination of access in these cases will result in two violations for the same error. We recommend that this issue be reconciled.

Likes 0

Dislikes 0

**Response**

**Jose Avendano Mora - Edison International - Southern California Edison Company - 1**

**Answer**

**Document Name**

**Comment**

See comments submitted by Edison Electric Institute

Likes 0

Dislikes 0

**Response**

**Thomas Standifur - Austin Energy - 1,3,4,5,6**

**Answer**

**Document Name**

[TPWR\\_2019-02\\_Unofficial\\_Comment\\_Form\\_2021-05-10.docx20210504-17090-hsevrj.docx](#)

**Comment**

Likes 0

Dislikes 0

**Response**

## Comments received from Basin Electric Power Cooperative

1. *The standards drafting team (SDT) considered industry’s concerns about the phrase “provisioning of access” requesting clarity on this terminology. The SDT added “authorize, verify, and revoke provisioned access” to the parent requirement CIP-004-X, Requirement R6, and changed “provisioning of access” to “provisioned access” in the requirement parts. This should clarify the intent that it is a noun which scopes what the Registered Entity must authorize, verify, and revoke, rather than a verb relating to how provisioning should occur. That is up to the entity to determine. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.*

Yes

No

**Comments:** The term “provisioned access” adds another undefined term to the NERC standards and doesn’t provide a clear path to regulatory off-prem or cloud data center services as proposed in the SAR. The only methods to control access to off-prem (cloud) BCSI is either by 1) encrypting BCSI or 2) purchasing services which allow the entity to manage the off-prem authentication systems – thereby preventing 3<sup>rd</sup> party systems administrators or others from compromising entity BCSI stored in cloud data centers. Option 2 is highly unlikely.

- a. “Provisioned access” creates a security loophole whereas entities only require authorization for a provisioned access. For example, if access to BCSI is not provisioned, no authorization to BCSI is required. This does not meet the goal of SAR for controlling access to BCSI. Given the R6 definition whereas “access to BCSI” occurs when an individual has both “the ability to obtain and use BCSI,” we recommend changing “provisioned access” to “access to BCSI”.
- b. The term “unless already authorized according to Part 4.1” should be removed. Why? Because having authorized access to CIP Cyber Assets does not preclude the authorization for having access to BCSI.
- c. The use of “provisioned, provision or provisioning” of “access,” regardless of tense, would require entities to be audited to, maintain, and provide documented lists of people and the “provisioned” configurations of entity BES Cyber System Information repositories in order to “verify” the “authorization” of such provisioned access. The Measures section highlights this expectation where evidence may include individual records, or lists of whom is authorized. To achieve this evidence, entities would need to provide evidence of systems accounts of on-premises or off premises system repositories of BCSI. Cloud providers will not provide such lists of personnel who have administrative level access to cloud BCSI server repositories and entities will be unable to verify what 3<sup>rd</sup> party off-prem systems administrators have access to BCSI, yet entities will be asked to provide this information for an entire audit cycle
- d. The current language requiring entities to 1) identify repositories and 2) authorize access based on need can also work for 3<sup>rd</sup> party off-prem or cloud locations without requiring lists of personnel or configurations of systems accounts for repositories of BCSI. (see recommendations)

### Recommendations:

1. Focus only on addressing electronic and physical access to BCSI in off-prem or cloud situations.
2. Consider the following language for R6 Part 6.1:

Authorize access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances. Access to BCSI includes:

6.1.1. Electronic access to electronic BCSI;

6.1.2 Physical access to physical BCSI;

6.1.3 Physical access to unencrypted electronic BCSI (See our comments in Q4).

3. Consider using the perspective of language in CIP-011 “to prevent unauthorized access to BES Cyber System Information.” This allows entities to determine the risk and methods to protect BCSI
  4. Consider using “authentication systems or encryption of BCSI” for personnel accessing electronic BCSI on cloud prem providers locations.
2. *The SDT considered industry’s concerns about the absence of “obtain and use” language from the CMEP Practice Guide, which currently provides alignment on a clear two-pronged test of what constitutes access in the context of utilizing third-party solutions (e.g., cloud services) for BCSI. The SDT mindfully mirrored this language to assure future enforceable standards are not reintroducing a gap. Do you agree this clarifying language makes it clear both parameters of this two-pronged test for “obtain and use” must be met to constitute “access” to BCSI? If not, please provide the basis for your disagreement and an alternate proposal.*

Yes

No

**Comments:**

- a. We agree to adding “obtain and use” language to clarify what constitutes an access to BCSI, but disagree to the use of “provisioned access”. After clarifying the access to BCSI, the language “provisioned” should be removed since it has a security flaw and requires extensive records from repositories of BCSI (See our comments in Q1).

**Recommendations:**

1. Only use the term “access” as recommended in Q1
3. *The SDT considered industry comments regarding the removal of storage locations. The SDT must enable the CIP standards for the use of third-party solutions (e.g., cloud services) for BCSI, and retention of that language hinders meeting those FERC directives. The absence of this former language does not preclude an entity from defining storage locations as the method used within an entity’s access management program. CIP-004-X, Requirement R6, is at an objective level to permit more than that one approach. Do you agree the requirement retains the flexibility for storage locations to be used as one way to meet the objective? If not, please provide the basis for your disagreement and an alternate proposal.*

Yes

No

**Comments:**

- a. We agree to retaining the flexibility for storage locations to be used as one way to meet the objective of SAR, but disagree to using “provisioned access” (See our comments regarding “provisioned access” in Q1).

- b. The requirement to provide lists of personnel with “provisioned access” would also require entities to identify the locations of BCSI and by auditors whom are required to make the link between the repository of BCSI which has been provisioned for access.

**Recommendation:**

Retain the current language and focus on auditable methods to protect BCSI at 3<sup>rd</sup> party off-prem (cloud) locations.

4. *To address industry comments while also enabling entities to use third-party solutions (e.g., cloud services) for BCSI, in CIP-004-X, Requirement R6 Part 6.1, the SDT made a distinction between “electronic access to electronic BCSI” versus “physical access to physical BCSI”. This clarifies physical access alone to hardware containing electronic BCSI, which is protected with methods that do not permit an individual to concurrently obtain and use the electronic BCSI, is not provisioned access to electronic BCSI. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.*

Yes

No

**Comments:**

We disagree that the physical access only applies to physical BCSI since controlling access to unencrypted BCSI has not been addressed but will be required for 3<sup>rd</sup> party off-prem (cloud) repositories. The physical access to Cyber Assets is a fast avenue to owning the unencrypted electronic BCSI it contains, which meets “obtain and use” condition and constitutes an access to BCSI.

**Recommendation:**

Adding “Physical access to unencrypted electronic BCSI” to R6 Part 6.1.3 (See our suggested R6 Part 6.1 changes in Q1).

5. *The SDT considered industry comments about defining the word “access”. “Access” is broadly used across both the CIP and Operations & Planning Standards (e.g., open access) and carries different meanings in different contexts. Therefore, the SDT chose not to define “access” in the NERC Glossary of Terms. Instead, the SDT used the adjective “provisioned” to add context, thereby scoping CIP-004-X, Requirement R6. Do you agree the adjective “provisioned” in conjunction with the “Note” clarifies what “provisioned access” is? If not, please provide the basis for your disagreement and an alternate proposal.*

Yes

No

**Comments:**

- a. Given that the SDT has defined “access to BCSI” in R6, and the term “provisioned access” should be removed due to the creation of an unintended security loophole (See our comments in Q1).
- b. Access, which occurs in CIP standards language, whether it is electronic and/or logical access, physical access, unescorted physical access, remote access, or interactive remote access is clearly understood, has been widely adopted by industry and regulators, and has been subject to hundreds of audits across all regions for the past 14 years. Entities have developed internal documentation, configured systems, implemented controls tasks and standardized programs on these terms. The adjective “provisioned” adds

further terms, requires changes and is of little value regarding the actions required of entities and the output deliverables or evidence.

**Recommendation:**

1. Revise the language to focus on access to BCSI and the auditable methods to protect BCSI at 3<sup>rd</sup> party off-prem (cloud) locations.
6. *In response to industry concerns regarding double jeopardy or confusion with CIP-013, the SDT removed CIP-011-X, Requirement R1 Parts 1.3 and 1.4, in favor of simplifying CIP-011-X, Requirement R1 Part 1.1, and adjusting Part 1.2 to broaden the focus around the implementation of protective methods and secure handling methods to mitigate risks of compromising confidentiality. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.*

- Yes  
 No

**Comments:** does not explain Prior language in the Rationale for Modifications to Requirement R1, Part 1.2 “By removing this language, methods to protect BCSI becomes explicitly comprehensive.”

7. *The SDT extended the implementation plan to 24-months in an attempt to align with the Project 2016-02 modifications that are on the same drafting timeline, and added an optional provision for early adoption. Do you agree this approach gives industry adequate time to implement without encumbering entities who are planning to, or are already using, third-party solutions (e.g., cloud services) for BCSI? If not, please provide the basis for your disagreement and an alternate proposal.*

- Yes  
 No

Comments:

8. *In looking at all proposed recommendations from the standard drafting team, are the proposed changes a cost-effective approach?*

- Yes  
 No

Comments:

9. *Please provide any additional comments for the SDT to consider, if desired.*

**Comments:**

1. Resulting from our comments in Q1, we suggest changing “provisioned access” to “access to BCSI” for whole R6 and its parts. Except our suggested changes to R6 Part 6.1, we also have the following recommendations for R6 Part 6.2 and 6.3:
  - For changes to R6 Part 6.2:

Verify at least once every 15 calendar months that all individuals with access to BCSI:  
6.2.1. have an Is authorization record;

6.2.2. Is still need the access to BCSI to perform their current work functions, appropriate based on need, as determined by the Responsible Entity.

- For changes to R6 Part 6.3:

For termination actions, remove the individual’s ability to 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.

We believe “access to BCSI” provides the flexibility for authorizing, verifying, and revoking access” to BCSI using various approaches including BCSI repositories and BCSI files, which make the R6 backwards compatible.

**2. The SDT may consider cleaning up the language to potentially the following language:**

R6. Each Responsible Entity shall implement an access management program(s) to authorize, verify, and revoke access to 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 CIP004-X Table R6 – Access Management for BES Cyber System Information.

[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]

Part	Revised Language Recommendations
6.1	Prior to authorization (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. Electronic access to electronic BCSI; and 6.1.2. Physical access to physical BCSI. Note: 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)
6.2	Verify at least once every 15 calendar months that all individuals with access to BCSI: 6.2.1. Have a current authorization record; and 6.2.2. A justification for authorization to perform their current work functions, as determined by the Responsible Entity.