Comment Report

Project Name:	2019-02 BES Cyber System Information Access Management (Draft 2)
Comment Period Start Date:	8/6/2020
Comment Period End Date:	9/21/2020
Associated Ballots:	2019-02 BES Cyber System Information Access Management CIP-004-7 AB 2 ST 2019-02 BES Cyber System Information Access Management CIP-011-3 AB 2 ST 2019-02 BES Cyber System Information Access Management Implementation Plan AB 2 OT

There were 68 sets of responses, including comments from approximately 175 different people from approximately 111 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree the revisions to CIP-004 clarify the requirements for managing provisioned access to BCSI when utilizing third-party solutions (e.g., cloud services)?

2. Do you agree the revisions to CIP-004 clarify that entities are only required to manage the provisioning of physical access to physical BCSI and electronic access to electronic BCSI?

3. Do you agree the revisions to CIP-011 clarify the protections expected when utilizing third-party solutions (e.g., cloud services)?

4. Do you agree the new and revised VSL/VRF descriptions clearly align with the revisions to CIP-004 and CIP-011?

5. The SDT is proposing an 18-month implementation plan. Do you agree to the proposed timeframe?

6. The SDT proposes that the modifications in CIP-004 and CIP-011 meet the project scope in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

7. Provide any additional comments for the standard drafting team 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
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
Midcontinent ISO, Inc.	Bobbi Welch	2	MRO,RF,SERC	ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management	Bobbi Welch	MISO	2	RF
					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
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Mark Holman	PJM Interconnection, L.L.C.	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
Douglas Webb	Douglas Webb		MRO,SPP RE	Westar-KCPL	Doug Webb	Westar	1,3,5,6	MRO
					Doug Webb	KCP&L	1,3,5,6	MRO
ACES Power Marketing	Jodirah Green	1,3,4,5,6			Bob Solomon	Hoosier Energy Rural Electric	1	SERC

			MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations		Cooperative, Inc.		
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Nick Fogleman	Prairie Power Incorporated	1,3	SERC
					Frank Owens	Rayburn Country Electric Cooperative, Inc.	3	Texas RE
					Jim Davis	East Kentucky Power Cooperative	1,3	SERC
					Carl Behnke	Southern Maryland Electric Cooperative	3	RF
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
Lincoln Electric System	Kayleigh Wilkerson	5		Lincoln Electric System	Kayleigh Wilkerson	Lincoln Electric System	5	MRO
					Eric Ruskamp	Lincoln Electric System	6	MRO
					Jason Fortik	Lincoln Electric System	3	MRO
					Danny Pudenz	Lincoln Electric System	1	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
Northern California Power Agency	Marty Hostler	5		NCPA	Michael Whitney	Northern California Power Agency	3	WECC
					Scott Tomashefsky	Northern California Power Agency	4	WECC
					Dennis Sismaet	Northern California Power Agency	6	WECC
					Marty	Northern California Power Agen	5	WECC
Duke Energy	Masuncha 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		PUD No. 1 of Chelan County	Ginette Lacasse	Public Utility District No. 1 of Chelan County	1	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Meaghan Connell	Public Utility District No. 1 of Chelan County	5	WECC
					Glen Pruitt	Public Utility District No. 1 of Chelan County	6	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 -	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company -	1	SERC

Southern Company Services, Inc.						Southern Company Services, Inc.		
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	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
					Michele Tondalo	UI	1	NPCC
					Helen Lainis	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					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
Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
Chantal Mazza	Hydro Quebec	2	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	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
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 Gas and Electric Co.	1	MRO
					Donald Hargrove	OGE Energy - Oklahoma Gas and Electric Co.	3	MRO
					Patrick Wells	OGE Energy - Oklahoma Gas and Electric Co.	5	MRO
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Jeff Neas	Sho-Me Power Electric Cooperative	3	SERC

					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. Do you agree the revisions to CIP-004 clarify the requirements for managing provisioned access to BCSI when utilizing third-party solutions (e.g., cloud services)?

Kjersti Drott - Tri-State G and T Association, Inc. - 1

Answer	No
Document Name	

Comment

Tri-State does not agree with all of the revisions.

The measures for R6.2 are too detailed when referring to privileges. Many types of access to BCSI are binary, either you have it or you do not. Recommend the SDT remove the 3rd and 4th bullets in the measure so that an entity could simply verify that the access is still necessary and appropriate for their job.

Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

The SDT should consider either defining the term “provisioned access” or removing it altogether in CIP-004 R6. The use of an undefined term such as “provisioned access” may lead to misunderstanding of the Standard and therefore may lead to inconsistent audit results. If you take “provisioned access” to mean only intentionally created individual accounts then administrative access to BCSI will not be governed by any Standard.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No
Document Name	

Comment

The addition of requirement 6 for CIP-004 makes it extremely difficult for entities to control access to BCSI. This is because of the requirement to provision access to individual pieces of information rather than provisioning access to where information is being stored (Storage locations).

We do not see how the changes clarify any requirements related to third-party solutions such as cloud services. Was the thought of changing the Applicability wording from "BCSI associated with" to "BCSI pertaining to" would provide the clarity that is being referenced? It is not obvious where any clarity is provided.

Likes 2	American Public Power Association, 4, Cashin Jack; Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

It is unclear in which instances provisioned access is applicable. Suggest include examples to clarify applicability by scenario (i.e.: cloud services).

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

For R6.1, the wording "based on need" is not necessary. SRP is not aware of any other reason that access would be authorized or than the fact there is a need for it. When access is authorized the fact there is a need is implied in the authorization. If it stays, how will you audit what is a valid "need"? If SRP authorizes access to everyone in a particular organization because SRP needs to comply with this requirement, is compliance a valid need? The focus should be on unauthorized access not appropriate business need.

For R6.1, the statement, "except for CIP Exceptional Circumstances" is not necessary. It's not clear if the exclusion "except for CIP Exceptional Circumstances" is stating in an Exceptional Circumstance it is not necessary to have business need or if it is not necessary to have authorization. (need to clarify) Even in an Exceptional Circumstance someone should still authorize the access – even though it might not follow the normal processes, at some level there is authorization, even if verbal.

For R6.1, in Measures, the statement "Dated authorization records for provisioned access to BCSI based on need". The statement based on need is not necessary here. If it is, then be clear on the expectations that the evidence needs to document the business need.

For R6.2, the wording “based on need” is not necessary. SRP supports requiring that the access “is authorized and appropriate as determined by the Responsible Entity.”

For R6.2, in Measures, if the requirement is to “Verify access to BCSI is appropriate based on needs” then why are the Measures silent on business need. Either remove business need or provide clarity on what is expected.

For R6.2, in Measures, the concept of “privileges” is not in CIP-004 R6, so it’s not clear how privileges will show compliance with the requirement. The Technical Rationale document states “Requirement 6.2 has been drafted to ensure the Responsible Entity reviews provisioned access **privileges** to BES Cyber System Information at least every 15 calendar months.” SRP does not see that in the R6.2 requirements.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	

Comment

The change from BCSI storage locations to personnel with provisioned access to BCSI creates a significant administrative overhead for entities and is not practical resulting in no security value. The BCSI repository is the key for controlling access to BCSI and it is impossible to authorize and provision access to each single piece of BCSI. CIP-011 should require all BCSI must be stored within a repository in the first place. When a BCSI is taken outside BCSI repository for use, this should fall within CIP-011 on how to protect and handle BCSI. The current CIP-004 R4 and R5 has addressed the third-party storage issue as long as the third party is willing to provide evidence for compliance with CIP-004 R5 and R4. Resulting from lack of alternative controls for meeting CIP-004 requirements, the goal of the SAR is to create increased choices for utilization of modern third-party data storage and analysis systems. but the change from BCSI storage locations to provisioned access doesn’t resolve the issues and causes more confusion. We suggest the following wording for CIP-004 R6.1 based on the example 3 of SAR:

Process to authorize based on need, as determined by the Responsible Entity, except for CIP

Exceptional Circumstances:

6.1.1. Physical access to physical BCSI Repository;

6.1.2. Physical access to unencrypted electronic BCSI Repository;

6.1.3. Electronic access to unencrypted electronic BCSI Repository; and

6.1.4. Electronic access to BCSI encryption keys for encrypted BES Cyber System Information.

The above wording The Part 6.14 can fit cloud storage services well. We suggest defining the BCSI Repository term and requiring BCSI Repository identification in CIP-011.

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	No
Document Name	
Comment	
Puget Sound Energy supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	
We do not understand all of the implications of the new term “provisioning.” Until we better understand these implications and expectations, we are concerned. Not sure how these changes address our concerns with the third party access Not sure how the addition of another list helps - - - appears to be more work. Especially for physical security Request clarification whether the third party access should be managed on an individual basis or on the team	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
Answer	No
Document Name	
Comment	
The intent of this standard development project was to enable entities to utilize third party service providers for storage and analysis of BCSI by defining the security control requirements should entities choose to utilize third party services. Utilizing third party providers may result in increased reliability, increased choice, greater flexibility, higher availability, and reduced-cost for entities. Current CIP standards essentially do not address this scenario.	

The SDT introduced a requirement to develop and implement an access management program for BCSI brought forward as a new requirement (a new R6 and previous R4.1.3, R4.4 and R5.3 are moved to the new R6) in the proposed CIP-004-7. Controls introduced as part of this program are similar to that of access management for electronic and unescorted physical access to BES Cyber Systems.

The addition of Requirement R6 in the proposed CIP-004-7 (draft 2) has introduced additional access management controls applicable to all scenarios including those who manage their BCSI without utilizing third party. We believe requiring additional security controls outside of the context of utilizing a third party is out of scope of this project.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

PAC does not agree with the revisions. The proposed revisions does not clarify the protections expected when utilizing third- party solutions (e.g., cloud services). The wording of requirement 6.2 expands the scope of the 15-month review by making it similar to the 4.2 quarterly requirement – verify that provisioned access is authorized. The requirement should be the same as CIP-004-6 R4.4 – verify that accesses are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.

PacifiCorp appreciates the change to the applicability to be consistent with the current version of the requirement.

We do believe this still allows for provisioned access to designated BCSI storage locations.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

The applicable portion of the control is R6.1, which BPA believes is very broad and lacking specificity in its wording: “Authorize provisioning of access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances.” The SDT must continue to consider the

physical storage of printed materials as well, so as not to exclude the possibility of protecting physical storage locations under some facsimile of the current methodology.

Proposed change:

Authorize provisioning of access to BCSI as follows:

R6.1.1 Authorize physical access to physical BCSI based on need, except for CIP Exceptional Circumstances; and

R6.1.2 Authorize electronic access to electronic BCSI (including BCSI maintained by, stored at, or shared with a vendor for purposes of analysis) based on need, except for CIP Exceptional Circumstances.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

1. There are very clear distinctions and limitations on the concept of what 'provisioned access' to BCSI constitutes and what it does not within the associated CIP-004-7 Technical Rationale document as drafted by the Standard Drafting Team. However, as this is not part of the CIP-004-7 standard itself, there is no guarantee that the Technical Rationale document guidance will be used as part of the compliance monitoring/enforcement approach, as regional enforcement agencies typically audit to the language of the standard. BC Hydro recommends that this clarity be incorporated directly into the CIP-004-7 standard requirements language to alleviate the risk of unintended interpretations in practice.
2. Require clarity as to whether CIP-004-7 Requirement 6 only applies to BCSI to which the Responsible Entity has the ability to directly control the provisioning of access and not to third-party service provider created or controlled repositories of BCSI (i.e. cloud services). For example, does this requirement apply to system administrators or support staff employed by a cloud service provider, or only to personnel with provisioned access to BCSI who are employed (either directly as employees/contractors or indirectly as sub-contractors) and who are terminated by the Responsible Entity?
3. Pending the answer to b), per CIP-004-7 Requirement 6.3, does the termination concept also apply to the cloud service provider's staff (or any other third-party service provider agency's staff members for that matter) and/or any of their sub-contractors who may be supporting a cloud service containing BCSI or managing a repository outside of the Responsible Entity's control?
4. The language of CIP-004-7 Requirement 6.2 only talks to the verification every 15 calendar months of provisioned access to BCSI (for authorizations and that access is appropriate based on need). The Measures however discuss the collection of evidence regarding specific privileges associated with authorizations and to compare against specific privileges that are provisioned as well. The concept of privilege reviews (i.e. least privilege) is also backed by the CIP-004-7 Technical Rationale document. This requirement needs further clarity to confirm whether 15-calendar month verifications are actually required to examine specific access privileges in addition to authorizations based on need or whether verifications of authorizations based on need is sufficient. If this is expected, should clarity that 'access privileges are appropriate based on need' be added to the standard requirement language.

Likes 0	

Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	

The change from authorizing designated storage location access to “provisioned access to BCSI” does not clarify the requirements, especially since “provisioned access” is not a defined term. While the term has changed from designated storage locations to “provisioned access,” the meaning seems to be the same when you review information in the technical rationale. The change in the term creates significant administrative work to update program documentation, as well as access tracking tools, without commensurate improvement or flexibility in security controls.

In addition, the wording of requirement 6.2 expands the scope of the 15-month review by making it similar to the 4.2 quarterly requirement – verify that provisioned access is authorized. The requirement should be the same as CIP-004-6 R4.4 – verify that accesses are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.

MidAmerican Energy Company appreciates the change to the applicability to be consistent with the current version of the requirement.

Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

The change from authorizing designated storage location access to “provisioned access to BCSI” does not clarify the requirements, especially since “provisioned access” is not a defined term. While the term has changed from designated storage locations to “provisioned access,” the meaning seems to be the same when you review information in the technical rationale. The change in the term creates significant administrative work to update program documentation, as well as access tracking tools, without commensurate improvement or flexibility in security controls.

In addition, the wording of requirement 6.2 expands the scope of the 15-month review by making it similar to the 4.2 quarterly requirement – verify that provisioned access is authorized. The requirement should be the same as CIP-004-6 R4.4 – verify that accesses are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.

MidAmerican Energy Company appreciates the change to the applicability to be consistent with the current version of the requirement.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC (CEHE) feels that Requirement R6 and its subparts do not provide clarity that one intent of these requirements is to manage access when utilizing third-party solutions since it doesn't explicitly make that statement. The phrase "provisioning of access" does not necessarily imply "when utilizing third party solutions." It is also ambiguous enough that it creates the impression that the phrase needs to be defined.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5, Group Name NCPA

Answer	No
Document Name	

Comment

See Tristate (SAR originator) and SMUDs comments.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

PG&E believes the modifications are a good step in clearly indicting that access to BCSI must be defined for the BSCI and not storage locations as indicated under the current Standards. These changes would make use of third party service providers (i.e. vendor or cloud) possible, but the language of Requirement Part 6.1 is confusion. Is an Entity authorizing provisioning of access or provisioning authorized access. The Technical Rational (TR) document has the following for R6:

"Methods to document and track authorization for access where provisioning of access is a prerequisite of being able to obtain and/or use the BES Cyber System Information"

The above is clearer than the Requirement language in P6.1, but the TR is not the Standard and should not be counted on when audit teams start their interruption of the Standard. PG&E recommends the language for Part 6.1 be modified to more clearly indicate in the intent, such as:

"Provisioning of authorized access to physical and electronic BCSI based on need as determine by the Responsible Entity, except for CIP Exceptional Circumstances."

PG&E also indicates physical and electronic should be indicated in P6.2 and P6.3

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Dominion Energy supports the comments 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	No
Document Name	

Comment

N&ST notes the proposed revisions say nothing at all about third-party solutions, cloud-based or otherwise.

Likes 0	

Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	
Oklahoma Gas & Electric supports the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
We support NPCC comments: We do not understand all of the implications of the new term “provisioning.” Until we better understand these implications and expectations, we are concerned. Not sure how these changes address our concerns with the third party access Not sure how the addition of another list helps - - - appears to be more work. Especially for physical security Request clarification whether the third party access should be managed on an individual basis or on the team	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	

Comment
We do not agree that the revisions in CIP-004 clarify the requirements for managing provisioned access to BCSI when utilizing third-party solutions. There is no mention of utilization of third-party solutions such as cloud services or vendor services in the requirements and or technical rationale in regards to question 1 above: https://www.nerc.com/pa/Stand/Project201902BCSIAccessManagement/2019-02_CIP-004-7_Technical_Rationale.pdf https://www.nerc.com/pa/Stand/Project201902BCSIAccessManagement/2019-02_CIP-004-7_redline_to_last_posted.pdf Further, the requirements in CIP-011 use the term “vendor services”, which does not match the way question 1 is framed. The new technical rationale assumes BCSI is outside of the Responsible Entity’s direct control, but with electronic mechanisms implemented to protect BCSI via CIP-011 R1.4, BCSI would in fact be in the Responsible Entity’s direct control. The new technical rationale goes on to explain: “For example, there is no available or feasible mechanism to provision access in instances when an individual is merely given, views, or might see BES Cyber System Information, such as when the individual is handed a piece of paper during a meeting or views a whiteboard in a conference room.” Simply being able to view BCSI in a meeting, on a screen, etc., does not constitute access. To access something in which access is controlled, such as under a CIP-011 Information Protection Program, requires credentials with provisioned privileges, such as a key, username/password, encryption key, badge, fingerprint, etc. and provisioned permissions to gain access. The new technical rationale is confusing provisioning with credentials: “Provisioning should be considered the specific actions taken to provide an individual the means to access BES Cyber System Information (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys).” A process to grant access, contains the element of provisioning which is part of the considerations of need to know/access. When an access request is processed, physical access as an example, an individual isn’t given access to every PSP unless requested. If access to all PSPs were requested, the request would be reviewed for need, and approved or denied based on need. If approved, the individual would be provisioned with those access rights and credentials given to access the PSPs. The process of granting of access is the full complement of, request, assessing need, approval, provisioning, and credentials. Access revocation can be achieved by the removal of ALL provisioned access rights or disabling of credentials. Access can be reduced or increased by provisioning of rights. In CIP-004-6’s Guidelines and Technical Basis, page 44 states: “Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked.”

The converse of revocation of access would be granting of access. The process of granting of access would result in providing individual(s) credentials with provisioned access privileges to access a BES Cyber System. Therefore we do not agree with the use of "provisioned access".	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	
APPA does not agree with the revisions to CIP-004. While public power supports that the revisions do not limit third party solutions, we also believe that the revisions are unclear about the requirement's applicability when using third-party solutions. APPA utilities want to be able to use third party solutions without unecessary regulatory risk.	
Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
Comments: GSOC greatly appreciates the SDT's consideration of its previous comments regarding the consolidation of all access management related requirements into CIP-004. However, it does not support the revisions to CIP-004 to clarify the requirements for managing provisioned access to BCSI when utilizing third-party solutions – as proposed – and provides the following comments for the SDT's consideration: 1. **Modification of Established Format -** As stated in its previous comments, while GSOC understands what the SDT was attempting to accomplish, it does not agree with the replacement of "Applicable Systems" with "Applicability." "Applicability" is already utilized in each of the reliability standards to denote whether or not a particular registered function has responsibility under the Standard. Utilization of the same term, but with a different scope of applicability within body of CIP-004 will result in confusion and ambiguity regarding the overall applicability of this reliability standard. Further, this change results in this Standard and CIP-011 (where this change has also been proposed) being different from the remaining CIP reliability standards relative to the CIP reliability standards overall approach to identification of asset scope. GSOC raises, for the SDT's consideration, that the deviation from the established format and scoping mechanisms used throughout the CIP reliability standard will create confusion and ambiguity and that any value achieved by this change will be far outweighed by the continued value associated with the current format and terms. To address this concern, GSOC proposes that the lead in requirement language for requirement R6 be modified as follows: Each Responsible Entity shall implement one or more documented access management program(s) for BES Cyber System Information ***about the "Applicable Systems" identified in CIP-004-7 Table R6 – Access Management for BES Cyber System Information*** that collectively include each	

of the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].

2. **Potential Scope Expansion -** GSOC notes that it is also concerned that the modifications to the contents of the "Applicability" column may potentially expand and obscure the established definition of BCSI set forth in the Glossary of Terms Used in NERC Reliability Standards. Specifically, the revisions limit the "applicability" to "BCSI associated with …" BCSI is defined as

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

The use of the term "associated with" is subjective and could be interpreted broadly by some entities and/or regulators. As an example, information about an external firewall configuration that acts as a first line of defense, but is not part of an applicable system, may contain information that "could be used to gain unauthorized access or pose a security threat to the BES Cyber System." It is unclear under the proposed revisions to the applicability column whether this information would be considered subject to CIP-004 – even if the asset from which it came is not in scope for any other reliability standards. This potential scope expansion and the associated ambiguity between the scope of CIP-004, the remaining reliability standards, and the Glossary of Terms Used in NERC Reliability Standards could result in increased compliance obligations without an attendant security or reliability benefit, confusion, and inconsistency of implementation. The proposed revision above would resolve this issue while preserving the current format of CIP-004 and its consistency with the remaining reliability standards.

3. Less flexibility/More restrictive language - As GSOC understands the draft, the objective of developing a dedicated requirement for access authorization to BCSI was to add flexibility for entities utilizing hosted services for BCSI storage, use, transit, etc. GSOC appreciates this objective and respectfully questions why the SDT utilized significantly different language in this requirement than the current "boilerplate" language utilized in the existing access authorization requirements – especially considering that the new language appears to be more restrictive. As an example, the current access authorization requirement language reads as follows:

Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter; …

The new language in requirement R6.1 reads as follows:

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

In requirement R6, the flexibility afforded to entities to define and implement an access authorization process (which may or may not specifically address provisioning depending on an entity's process and needs) has been removed and, although the technical rationale alludes to the ability to have no authorization or provisioning where such is not possible, the requirement, on its face, as proposed, does not appear to afford such flexibility.

Indeed, a plain reading of the requirement would indicate that access to any individual piece of BCSI would require authorized, provisioned access. For this reason, GSOC would respectfully suggest that this modification is unnecessarily restrictive and that the retention of the current boilerplate language (with minor revision) would afford Responsible Entities more flexibility to define their processes for both self-hosted and third-party hosted data within their BCSI program. For these reasons, GSOC recommends that the SDT revise the lead-in requirement language as indicated above and revise the proposed language for Requirement R6.1 to

Process to authorize access based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances

Finally, the value of driving consistency in rigor and format for access authorization must be considered. GSOC does not foresee that the value of changing the established format, applicability, and access-related obligations for one piece of the overall security framework that comprises the CIP reliability standards will outweigh the value of developing enhancements that conform with the established, known format, applicability, and access-related obligations currently in place.

4. Maintain consistency with established language – For the same reasons described above, GSOC would respectfully recommend that requirements R6.2 and R6.3 also be reverted to language similar to that currently utilized within the existing access management requirements, e.g.:

R6.2 Verify at least once every 15 calendar months that access to **BCSI or its designated storage location,** whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.

R6.3 For termination actions, revoke the individual's access to **BCSI or its designated storage location,** whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.

5. Backwards compatibility - GSOC appreciates the SDT's consideration of the important concept of backwards compatibility in the Technical Rationale; however, the shift from access authorization by repository/location or BCSI to BCSI only appears to remove the ability of Responsible Entities to manage such authorizations, verifications, and terminations based on the use of designated storage locations or repositories. Many current programs have been developed and are managed around the concept of repositories or storage locations – not individual pieces of BCSI. For this reason, GSOC cannot agree that the proposed requirements are actually backwards compatible nor that minimal effort will be required to meet these new requirements. In particular, the proposed requirements focus solely on each individual piece of information and the management of access thereto. The obvious implementation method to ensure compliance would be to create and maintain a list of each individual piece of BCSI, its location, and its format. Such a list would be a new development that would likely not be compatible with existing program implementations.

6. Technical Rationale as support for revisions - GSOC notes the Technical Rationale does not appear to be consistent with the proposed revisions and does not make a convincing case for the significant changes proposed, e.g., revision of the requirement structure, inability to manage BCSI by location or repository, etc. To address this, GSOC proposes the above revisions, which would maintain the current format and provide flexibility for the management of BCSI via documented processes that can address either individual BCSI management, management by repository/location, or both. To ensure consistency between the Technical Rationale and the proposed revisions, GSOC respectfully suggests that the SDT review these documents objectively and make necessary revisions.

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	No
Document Name	

Comment

SDG&E supports EEI's comments submitted on our behalf, and in addition, submits the following comments below regarding CIP-004-7 Requirement 6, part 6.1.

Discussions with the Standard Drafting Team (SDT) have clarified that CIP-004-7 R6.1 was not intended to require provisioning of access to each individual piece of BCSI. The SDT explained that the language was written to accommodate a use case where the BCSI authorization attaches to the document so that the authorization follows the document when moved to various locations.

To accommodate both circumstances where entities may fall under the use case scenario or may use designated storage locations for BCSI, SDG&E proposes the following two options:

1. Provide two parts to the requirement. One part will be similar to the current CIP-004-6 R4.1.3 which requires authorization of access to BCSI designated storage locations. The other part will authorize the provisioning of access to BCSI for documents not stored in a designated storage location.

2. Given the possibly low frequency of the described use case, retain the current CIP-004-6 R4.1.3 BCSI designated storage location authorization requirement while adding a provision to ensure that documents not stored in BCSI storage locations are protected according to the other CIP information protection requirements.

Two other alternatives are suggested below:

Proposal No. 1:

Authorize provisioning of access to BCSI based on need **and** as determined by the Responsible **Entity's designated method(s) to protect and securely handle BCSI**, except for CIP Exceptional Circumstances.

Proposal No. 2:

Using one or a combination of the following methods, authorize provisioning of access to BCSI 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; or**
- **Access to BES Cyber System Information, whether physical or electronic.**

If the SDT does not adopt any changes to the CIP-004-7 R6.1 Requirement language, please consider adding clarifying language in the Measures and/or Technical Rationale explicitly stating that authorization of access to BCSI is not required for each individual piece of BCSI.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO-NSRF comments.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

See Tristate (SAR originator) and SMUDs comments.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

NV Energy does not agree with the revisions. The proposed revisions does not clarify the protections expected when utilizing third-party solutions (e.g., cloud services). The wording of requirement 6.2 expands the scope of the 15-month review by making it similar to the 4.2 quarterly requirement – verify that provisioned access is authorized. The requirement should be the same as CIP-004-6 R4.4 – verify that accesses are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.

NV Energy appreciates the change to the applicability to be consistent with the current version of the requirement.

NVE also supports EEI's comments on providing clarity on the language associated with Requirement R6, Part 6.1, and aligning the language of Requirement R6, part 6.1 to Requirement R4, part 4.1 by adding the phrase “Process to”, which would place the responsibility on the entity to define its process.

Likes 0	
Dislikes 0	

Response

Larry Snow - Cogentrix Energy Power Management, LLC - 4 - NPCC,SERC,RF

Answer	No
Document Name	

Comment

The term "provisioning" is ambiguous and could lead to various interpretations of the requirements across the regions. More detailed clarification is needed of the term is to remain in the language. Concerns over 3rd party access control and what appears to be additional lists and documantation.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management	
Answer	No
Document Name	2019-02_Unofficial_Comment_Form_IRC SRC_FINAL_09-21-20.docx
Comment	

There is a lack of clarity around the implications of the new term “provisioning.” Until the ISO/RTO Council Standards Review Committee (IRC SRC) better understand these implications and expectations, we are concerned.

It seems like the SDT has attempted to break the process of providing access to BCSI into two component parts: The authentication process, which we are assuming is a much broader list, coupled with the technical controls that are being referred to in the standard as “provisioning.” The mandate would be that no user should be “provisioned” access without (first) being authorized. At first glance this seems to raise the compliance burden without providing any real security value.

It’s not clear to us how these changes are looking to facilitate the storage of BCSI by third party providers or even how the audit requirements would be met in the use case of utilizing cloud based services for the processing or storage of BCSI.

Another concern that we have is how this would be applied to physical controls on physical (non-electronic) documents.

We request clarification as to how third party access would be managed.

In lieu of additional work to define “provision,” we request the SDT consider eliminating requirement R6 and focus its efforts on modifying the existing language in requirement 4.1 using the examples from page 4 of the SAR as a starting point and making as few changes as possible to achieve the objectives. This would simplify the solution and streamline entity costs associated with transition. For example:

R4.1 Process to authorize ***the following*** based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

4.1.1. Electronic access;

4.1.2. Unescorted physical access into a Physical Security Perimeter;

4.1.3. ***Physical access to physical BES Cyber System Information storage locations;***

4.1.4. ***Physical access to unencrypted electronic BES Cyber System Information storage locations***;

4.1.5. ***Electronic access to unencrypted electronic BES Cyber System Information storage locations;***

4.1.6. ***Electronic access to BES Cyber System Information encryption keys for encrypted BES Cyber System Information***

[1] For purposes of these comments, the IRC SRC includes the following entities: CAISO, ERCOT, IESO, ISO-NE, MISO, NYISO, PJM and SPP.

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	No
Document Name	

Comment
We do not understand all of the implications of the new term “provisioning.” Until we better understand these implications and expectations, we are concerned. Not sure how these changes address our concerns with the third party access Not sure how the addition of another list helps - - - appears to be more work. Especially for physical security Request clarification whether the third party access should be managed on an individual basis or on the team The intent of this standard development project was to enable entities to utilize third party service providers for storage and analysis of BCSI by defining the security control requirements should entities choose to utilize third party services. Utilizing third party providers may result in increased reliability, increased choice, greater flexibility, higher availability, and reduced-cost for entities. Current CIP standards essentially do not address this scenario. The SDT introduced a requirement to develop and implement an access management program for BCSI brought forward as a new requirement (a new R6 and previous R4.1.3, R4.4 and R5.3 are moved to the new R6) in the proposed CIP-004-7. Controls introduced as part of this program are similar to that of access management for electronic and unescorted physical access to BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	

Comment
Management of provisioned access to BCSI, when utilizing third-party solutions, needs to be clarified. Requirement R6, part 6.1 states that entities are required to “authorize provisioning of access to BCSI based on need.” This could be read to mean, among other things, that entities are required to authorize someone to provision access to BCSI, provision access to all BCSI (i.e. requiring a provisioning authorization for each piece of BCSI), or a variety of other interpretations. To resolve this issue, EEI suggests aligning the language of Requirement R6, part 6.1 to Requirement R4, part 4.1 by adding the phrase “Process to”, which would place the responsibility on the entity to define its process. Additionally, EEI suggests adding the following “Measure” to Requirement 6, Part 6.1: • A documented process used to define provisioned access to BCSI.

Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Provisioned access terminology should be removed. When access revocation is necessary the provisioned access, as well as the authorization for access shall be removed.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
Please incorporate the guidance from the “Compliance Implementation Guidance Cloud Solutions and Encrypting BES Cyber System Information – June 2020” document into the CIP-004 and CIP-011 revisions.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
We support NPCC Regional Standards Committee comments	
Likes 0	

Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	

Comment

CAISO is in support of the below IRC SRC comments:

There is a lack of clarity around the implications of the new term “provisioning.” Until the ISO/RTO Council Standards Review Committee (IRC SRC)[1] better understands these implications and expectations, we are concerned.

It seems like the SDT has attempted to break the process of providing access to BCSI into two component parts: The authentication process, which we are assuming is a much broader list, coupled with the technical controls that are being referred to in the standard as “provisioning.” The mandate would be that no user should be “provisioned” access without (first) being authorized. At first glance this seems to raise the compliance burden without providing any real security value.

It’s not clear to us how these changes are looking to facilitate the storage of BCSI by third party providers or even how the audit requirements would be met in the use case of utilizing cloud based services for the processing or storage of BCSI.

Another concern that we have is how this would be applied to physical controls on physical (non-electronic) documents.

We request clarification as to how third party access would be managed.

In lieu of additional work to define “provision,” we request the SDT consider eliminating requirement R6 and focus its efforts on modifying the existing language in requirement 4.1 using the examples from page 4 of the SAR as a starting point and making as few changes as possible to achieve the objectives. This would simplify the solution and streamline entity costs associated with transition. For example:

R4.1 Process to authorize the following based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

4.1.1. Electronic access;

4.1.2. Unescorted physical access into a Physical Security Perimeter;

4.1.3. Physical access to physical BES Cyber System Information storage locations;

4.1.4. Physical access to unencrypted electronic BES Cyber System Information storage locations;

4.1.5. Electronic access to unencrypted electronic BES Cyber System Information storage locations; and

4.1.6. Electronic access to BES Cyber System Information encryption keys for encrypted BES Cyber System Information.

[1] For purposes of these comments, the IRC SRC includes the following entities: CAISO, ERCOT, IESO, ISO-NE, MISO, NYISO, PJM and SPP.

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	

We do not agree that the revisions in CIP-004 clarify the requirements for managing provisioned access to BCSI when utilizing third-party solutions. There is no mention of utilization of third-party solutions such as cloud services or vendor services in the requirements and or technical rationale in regards to question 1 above:
https://www.nerc.com/pa/Stand/Project201902BCSIAccessManagement/2019-02_CIP-004-7_Technical_Rationale.pdf

https://www.nerc.com/pa/Stand/Project201902BCSIAccessManagement/2019-02_CIP-004-7_redline_to_last_posted.pdf

Further, the requirements in CIP-011 use the term “vendor services”, which does not match the way question 1 is framed.

The new technical rationale assumes BCSI is outside of the Responsible Entity’s direct control, but with electronic mechanisms implemented to protect BCSI via CIP-011 R1.4, BCSI would in fact be in the Responsible Entity’s direct control.

The new technical rationale goes on to explain:

“For example, there is no available or feasible mechanism to provision access in instances when an individual is merely given, views, or might see BES Cyber System Information, such as when the individual is handed a piece of paper during a meeting or views a whiteboard in a conference room.”

Simply being able to view BCSI in a meeting, on a screen, etc., does not constitute access. To access something in which access is controlled, such as under a CIP-011 Information Protection Program, requires credentials with provisioned privileges, such as a key, username/password, encryption key, badge, fingerprint, etc. and provisioned permissions to gain access. The new technical rationale is confusing provisioning with credentials:

“Provisioning should be considered the specific actions taken to provide an individual the means to access BES Cyber System Information (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys).”

A process to grant access, contains the element of provisioning which is part of the considerations of need to know/access. When an access request is processed, physical access as an example, an individual isn’t given access to every PSP unless requested. If access to all PSPs were requested, the request would be reviewed for need, and approved or denied based on need. If approved, the individual would be provisioned with those access rights and credentials given to access the PSPs. The process of granting of access is the full complement of, request, assessing need, approval, provisioning, and credentials. Access revocation can be achieved by the removal of ALL provisioned access rights or disabling of credentials. Access can be reduced or increased by provisioning of rights. In CIP-004-6’s Guidelines and Technical Basis, page 44 states:

“Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked.”

The converse of revocation of access would be granting of access. The process of granting of access would result in providing individual(s) credentials with provisioned access privileges to access a BES Cyber System. Therefore we do not agree with the use of “provisioned access”.

Likes 0	
Dislikes 0	
Response	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern does not agree the revisions to CIP-004 provide enough clarity. While the Technical Rationale provides additional clarity, the enforceable requirement of "Authorize provisioning of access to BCSI based on need" is a virtually unlimited statement and is not scoped to where the BCSI is stored. It does not exclude BCSI in use. Entities cannot prove the prevention of "unprovisioned" personnel "accessing" BCSI such as hardcopies, or in discussions in a meeting. The Technical Rationale explicity acknowledges this dilemma, but those concepts do not make it to the enforceable language. We can provision access to BCSI where it is stored and with the loss of that concept within the language of the requirement, clarity is also lost.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	No
Document Name	
Comment	
ITC supports the Comment Form submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with EEI's comments to rephrase R6.1 to mirror 4.1, "Process to authorize access to BCSI based on need…" Also, the written requirement should be clear about the requirements for authorizing access to BCSI stored in the cloud. Is the expectation that encryption with key management be utilized? Is merely obtaining access lists of personnel from the vendor sufficient, when the requirement states to authorize "based on need, as determined by the Responsible Entity"? The concern is that if NERC is looking for encryption, will they find individual	

entities who do not utilize encryption for BCSI in the cloud to have insufficient security controls in place, even if they requirement is written so as not to prevent that scenario.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Bryan Taggart, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Grant Wilkerson, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Co, Evergy companies, incorporate by reference Edison Electric Institute's response to Question 1.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran

Answer	Yes
Document Name	

Comment

Oncor supports EEI's comment.

Likes 0	

Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Although the revision facilitates using a third-party solution, FEU suggests the SDT consider using a third-party example in the Measures of the new R6 requirements.	
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 supports the change from “designated storage locations” to “provisioned access”. It is backwards compatible, scopes applicability, clarifies requirements when utilizing cloud services, and better defines what access entities are expected to control. MPC also appreciates the use of the qualifier “provisioned” in front of the broad term “access” in R6, and the time invested in the technical rationale document and how it informs industry on what this qualifier means and does not mean. The broad term “access”, when used without context, has led to significant misinterpretation and unintended consequences of what constitutes “access to BCSI” vs “visibility/sharing of BCSI”, which makes the term “provisioned” an important differentiator and a good improvement.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

ATC appreciates the SDT's removal of BCSI from CIP-004-6 Requirements R4 and R5, and the result to keep this apart from the realm of physical access to where electronic BCSI may be physically stored, which has been a point of contention and confusion. Creating the new requirement R6 accomplishes this separation and clarity making it possible for the controls to not only be commensurate with risk, but also to be commensurate with the format of the BCSI and the types of methods available to protect digital vs hardcopy.

ATC also appreciates the use of the qualifier "provisioned" in front of the broad ranging term "access" in R6, and the time invested in the TR and how it informs industry on what this qualifier means and doesn't mean. The broad term "access" when used without context has led to significant misinterpretation and unintended consequences of what constitutes "access to BCSI" vs "visibility/sharing of BCSI" and making the term "provisioned" an important differentiator, and a good improvement.

ATC further appreciates how this proposed qualifier "provisioned" **scopes CIP-004** to that which the entity can **control**; meaning that access which we (the entity) authorizes, we can control what access we (the entity) provisions (configures).

- We cannot control another person's cognition and retention; and should not have requirements that misconstrue "see/hear/store in brain" as "access" as opposed to that invoking "handling protections for a business need to share on a temporary basis by a person with authorized provisioned access".
- Additionally, this approach helps prevent overreach in CIP-004 for controls on the "unauthorized access" side; Here, risk mitigation is more relevant. CIP-004 is about the controls to address the expected by providing the right access to the people who need it when they need it, and not about the logging, alerting, monitoring, prevention, detection, deterrence, and response measures that belong somewhere else outside of CIP-004 to address the unexpected. Mitigating controls like those in **CIP-011** are the ones that **help prevent** the "unauthorized access" from happening; which is very different than the intent of **CIP-004** which is to **control** the authorization and provisioning aspect.

CIP-004 – control what is in our control and manage authorized provisioned access

authorized = the people we expect to have access based on need;

provisioned = the people who are actually configured for that access;

provisioned can be a subset of authorized; an entity is not in violation if the list of authorized people is greater than the list of provisioned people as long as all who are provisioned are also authorized

CIP-011 – mitigate risk for that which we cannot completely control; an unauthorized individual gaining unauthorized access. By adding "provisioned" as a qualifier to CIP-004 access we scope the evidence further than it is today while also starting to remove the ability for industry to get dinged under CIP-004 for the unintended types of "access" that are on the wrong side of BOOM.

Likes 0	
Dislikes 0	

Response

Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6

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	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
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	
Kent Feliks - AEP - 3	
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	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
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	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,SERC,RF, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy needs more clarification on authorized provisioning as it applies to repositories versus discrete pieces of BCSI. Duke Energy would also like to know the difference between Authorized and Authorized provisioniong.Duke Energy needs more clarification on authorized provisioning as it applies to repositories versus discrete pieces of BCSI. Duke Energy would also like to know the difference between Authorized and Authorized provisioniong.	

Likes 1	Wabash Valley Power Association, 3, Sosbe Susan
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

Kinte Whitehead - Exelon - 3

Answer	
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	
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	
Document Name	
Comment
Exelon has elected to align with EEI in response to this question.
Likes 0	
Dislikes 0	
Response

2. Do you agree the revisions to CIP-004 clarify that entities are only required to manage the provisioning of physical access to physical BCSI and electronic access to electronic BCSI?

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Bryan Taggart, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Grant Wilkerson, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Co, Evergy companies, incorporate by reference Edison Electric Institute's response to Question 2.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Alliant Energy agrees with EEI's comments.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

ITC supports the Comment Form submitted by EEI

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	

We do not agree with the new language in R6's requirements, which does not distinguish between physical and/or electronic access to BCSI and could cause confusion. We also disagree with the use of "provisioning of." Part of the process of granting access is provisioning access such as read-only, read/write, etc. There is no need to change the verbiage used in CIP-004 for access, as it has been used in the standards for years and is clear. If adding "provisioning of" to access for BCSI it should be added to electronic access and physical access. Adding this would cause further confusion and ambiguity to the requirements.

Further, while not all measures are necessary to meet the requirement, the measures for R6.2 for entities trying to meet or exceed the requirement are administratively burdensome and duplicative with the clause "not limited to" in the evidence examples.

Likes 0	
Dislikes 0	
Response	

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	

CAISO is in support of the below IRC SRC comments:

There needs to be more clarification on what constitutes "provisioning."

Today, technical access controls are used as physical security provisioning. We are concerned as to how these requirements are intended to be applied to non-electronic BCSI.

The IRC SRC would request that the intent of "provisioning" be spelled out more explicitly in the Measures instead of the Technical Guidance - - - possibly in 6.1.

In lieu of additional work to define "provision," we request the SDT consider eliminating requirement R6 and focus its efforts on modifying the existing language in requirement 4.1 using the examples from page 4 of the SAR as a starting point and making as few changes as possible to achieve the objectives. This would simplify the solution and streamline entity costs associated with transition. For example:

R4.1 Process to authorize the following based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

4.1.1. Electronic access;

4.1.2. Unescorted physical access into a Physical Security Perimeter;

4.1.3. Physical access to physical BES Cyber System Information storage locations;

4.1.4. Physical access to unencrypted electronic BES Cyber System Information storage locations;

4.1.5. Electronic access to unencrypted electronic BES Cyber System Information storage locations; and

4.1.6. Electronic access to BES Cyber System Information encryption keys for encrypted BES Cyber System Information.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Please incorporate the guidance from the “Compliance Implementation Guidance Cloud Solutions and Encrypting BES Cyber System Information – June 2020” document into the CIP-004 and CIP-011 revisions.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Although the technical rationale provides clarity on this issue, the language contained in CIP-004-7 does not provide similar clarity. Given compliance is based on the plain language of the Reliability Standard, EEI suggests the following modifications to CIP-004-7to provide greater clarity:

Requirement R6

Part 6.1: Authorize provisioning of **physical access and/or electronic access** to BCSI **as appropriate and** based on need,….

Part 6.2: Verify at least once every 15 calendar months that provisioned access to **physical and/or electronic** BCSI **as appropriate**:

Part 6.3: For termination actions, remove the individual’s ability to use provisioned access to **physical and/or electronic** BCSI **as appropriate** (unless already revoked according to Part 5.1) by the ……

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

There needs to be more clarification on what constitutes “provisioning.”

Today, technical access controls are used as physical security provisioning. We are concerned as to how these requirements are intended to be applied to non-electronic BCSI.

The IRC SRC would request that the intent of “provisioning” be spelled out more explicitly in the Measures instead of the Technical Guidance - - - possibly in 6.1.

In lieu of additional work to define “provision,” we request the SDT consider eliminating requirement R6 and focus its efforts on modifying the existing language in requirement 4.1 using the examples from page 4 of the SAR as a starting point and making as few changes as possible to achieve the objectives. This would simplify the solution and streamline entity costs associated with transition. For example:

R4.1 Process to authorize ***the following*** based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

4.1.1. Electronic access;

4.1.2. Unescorted physical access into a Physical Security Perimeter;

4.1.3. ***Physical access to physical BES Cyber System Information storage locations;***

4.1.4. ***Physical access to unencrypted electronic BES Cyber System Information storage locations;***

4.1.5. ***Electronic access to unencrypted electronic BES Cyber System Information storage locations;***

4.1.6. ***Electronic access to BES Cyber System Information encryption keys for encrypted BES Cyber System Information***

Likes 0	
Dislikes 0	

Response

Larry Snow - Cogentrix Energy Power Management, LLC - 4 - NPCC,SERC,RF

Answer	No
Document Name	

Comment

Again, the term "provisioning" is troublesome and will create confusion and inconsistencies.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
NV Energy is aware that clarity on this topic ("...**manage the provisioning of physical access to physical BCSI and electronic access to electronic BCSI")** is provided within the supplemental Technical Rationale document for this Project, but this clarification should be added to the language of the requirement. Entities are audited to the plain language of the Standard, and not the Technical Rationale for the justification of a Requirement, so the CIP-004-7 should explicitly state that provisioning of access is for **physical access to physical BCSI and electronic access to electronic BCSI.** This will remove any ambiguity. Example would be to include the term, "physical access and/or electronic access to...", preceding BCSI in Part 6.1, 6.2, and 6.3	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
See SMUDs comments.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	

Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	No
Document Name	
Comment	
SDG&E supports EEI's comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
Comments: No. GSOC does not agree that the revisions to CIP-004 clarifies that entities are only required to manage the provisioning of physical access to physical BCSI and electronic access to electronic BCSI. If this is intended to be connoted by the introduction of the term "provisioned," GSOC would respectfully suggest that the insertion of that term is not enough to communicate the above concept and that the SDT consider additional revisions to clarify their intent. Further, GSOC is concerned that, the guidance in the Technical Rationale notwithstanding, the term "provisioned" is undefined. Accordingly, both the term and its associated activities could be both implemented and interpreted differently by various Responsible and Regional Entities. Finally, GSOC is concerned that the concept indicated above and the guidance provided in the Technical Rationale could leave a potential security gap around the management of BCSI. For example, what obligation do Responsible Entities have related to BCSI that is typically stored and managed electronically, but may be printed out or otherwise displayed? Conversely, where BCSI is typically stored and managed physically, but is converted to an electronic format to facilitate vendor or other review, what would a Responsible Entity's obligation be to authorize access thereto? GSOC appreciates that the SDT is trying to create flexibility around access management, but is concerned that the resulting ambiguity could create issues from both a security and compliance perspective.	
Likes 0	
Dislikes 0	

Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	

Public power does not agee that the CIP-004 revisions specifically separate the compliance between providing physical access to BES cyber system information and electronic access to BES cyber system information. The requirement language does not distinctly separate the treatment of physical versus electronic BES cyber system information. APPA recommends that language be added making this distinction between physical and electronic access clear.

APPA supports the suggested way the language could be revised provided by Tacoma Power in their 2019-02 comments:

"Authorize provisioning of physical access to physical BCSI and electronic access to electronic BCSI, based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances."

Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	

We do not agree with the new language in R6's requirements, which does not distinguish between physical and/or electronic access to BCSI and could cause confusion. We also disagree with the use of "provisioning of." Part of the process of granting access is provisioning access such as read-only, read/write, etc. There is no need to change the verbiage used in CIP-004 for access, as it has been used in the standards for years and is clear. If adding "provisioning of" to access for BCSI it should be added to electronic access and physical access. Adding this would cause further confusion and ambiguity to the requirements.

Further, while not all measures are necessary to meet the requirement, the measures for R6.2 for entities trying to meet or exceed the requirement are administratively burdensome and duplicative with the clause "not limited to" in the evidence examples.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

We support NPCC comments:

Need to nail down “provisioning” in order to answer Yes or No

Today’s technical access is the physical security provisioning.

Prefer the intent of “provisioning” to be in the Measures instead of the Technical Guidance - - - possibly in Part 6.1

Removing the notion of access to designated storage locations, whether physical or electronic reduces any ambiguity it may have had with respect to the management of physical access where the BCSI resides on a electronic form.

Emphasis could be placed on the concept introduced in the ERO Enterprise CMEP Practice Guide published on April 26, 2019 where access to the BCSI is defined by the individual ability to obtain and use the BCSI.

Depending on the security measures in place (e.g. encryption with key management), it makes it explicit that an individual with physical access to a data center containing BCSI, but without the ability to use the BCSI (due to encryption) would not be within the scope of the requirement.

For exemple:

6.1 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

Ability to obtain and use BCSI, wheter physical or electronic.

6.2 Verify at least once every 15 calendar months that all individual’s with ability **to obtain and use** BCSI:

6.2.1. Is authorized; and

6.2.2. Is appropriate based on need, as determined by the Responsible Entity

6.3 For termination actions, remove the individual’s ability to **obtain and use** 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.

Likes 0	
Dislikes 0	
Response	

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	

Oklahoma Gas & Electric supports the comments 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	No
Document Name	

Comment

N&ST believes the proposed revisions neither adequately define nor clearly convey what it means to "provision access" to BCSI. If someone is handed a piece of paper, on which is printed information classified as BCSI, has that individual been "provisioned" with "physical access to physical BCSI"? Similarly, has an individual been "provisioned" for "electronic access to electronic BCSI" if an electronic copy of that same document is sent to him or her via email? N&ST is concerned, based on 10 years of experience with compliance monitoring and enforcement programs, that if CIP-004 doesn't clearly define what "provisioning" means, audit teams will develop their own definitions (use of plural is intentional). N&ST recommends maintaining CIP-004's well-understood requirement to manage access to "designated storage locations," which may be electronic (e.g., a file server) or physical (e.g., a lockable file cabinet).

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The plain language of the Standard does not align with the language in the technical rationale for Requirement 6. DOminion Energy recommends the Requirement language be aligned with thetechnical rationale as follows:

Requirement R6

Part 6.1: Authorize provisioning of **physical access and/or electronic access** to BCSI **as appropriate and** based on need,….

Part 6.2: Verify at least once every 15 calendar months that provisioned access to

physical and/or electronic BCSI **as appropriate**:

Part 6.3: For termination actions, remove the individual's ability to use provisioned

access to **physical and/or electronic** BCSI **as appropriate** (unless already revoked according to Part 5.1) by the ……	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
While this is implied in the language of the Requirement R6 “Parts”, the lack of such words as physical or electronic does not make it clear the Requirements are for both. PG&E believes this lack of explicit reference to physical or electronic is problematic and should be corrected by clearly indicating the provisioning of access should be for physical and electronic BCSI as PG&E indicated in the answer to Question 1.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5, Group Name NCPA	
Answer	No
Document Name	
Comment	
See SMUDs comments.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	

The CIP-004 Requirement R6 requirement revisions do not provide the clarity that entities are only required to manage the provisioning of physical access to physical BCSI and electronic access to electronic BCSI. The following suggested modification would make it clear;

· Part 6.1: Authorize provisioning of physical access to physical BCSI and/or electronic access to electronic BCSI based on need, …

· Part 6.2: Verify at least once every 15 calendar months that provisioned access to physical and/or electronic BCSI: …

· Part 6.3: For termination actions, remove the individual's ability to use provisioned access to physical and/or electronic BCSI (unless already revoked according to Part 5.1) by the …

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Comments: No, this is not clear with the limited wording "provisioning of access." While there is additional information in the technical rationale, the requirement text itself does not clarify this point.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

No, this is not clear with the limited wording "provisioning of access." While there is additional information in the technical rationale, the requirement text itself does not clarify this point.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	

1. The CIP-004-7 Technical Rationale document do explain this concept however this is not clear from the standard language itself. BC Hydro recommends that the clarity provided per the Technical Rationale be incorporated into the actual standard language or be formally adopted as NERC endorsed implementation guidance to avoid misinterpretations as the enforcement agencies typically audit to the language of the reliability standards and not to these additional documents.
2. Within the CIP-004-7 Technical Rationale document, the SDT's intent around provisioning of electronic access to electronic BCSI is not clear. There is specific mention of the following:

"For BES Cyber System Information in electronic format, electronic access is provisioned to an electronic system's front-end interface regardless of the geographical or physical location of the server or storage device or to individual encrypted files. Provisioning physical access to a physical location or storage device that contains electronic BES Cyber System Information is not considered provisioning access to electronic BES Cyber System Information." Further explanation is required as to what is considered the front-end interface. For example consider a server hosting a SharePoint platform which in turn contains BCSI. What is/are considered the front-end interface(s) in this case? The server OS? The Sharepoint platform itself? This should be clarified within the language of the standard or incorporated into a NERC endorsed implementation guidance document instead of limited to a Technical Rationale document to avoid misinterpretations. Enforcement agencies typically audit to the language of the reliability standards and not to Technical Rationale documents.

Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
See BPA's comments to Question 1, above.	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
Answer	No
Document Name	

Comment
If the intent was to make clarification about explicitly mentioning physical and electronic access, the SDT will need to make further revisions to clarify that. CIP-004-6 is currently only require managing physical access to BCSI. The need to manage electronic access is not explicitly stated but falls under the requirement to protect BCSI under CIP-011-2 Requirement R1 and as part of entities' Information Protection program.

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	No
Document Name	

Comment
Puget Sound Energy supports the comments of EEI.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	

Comment
Managing the provisioning of physical access to physical BCSI is misleading. For instance, if all unencrypted BCSI are stored on a sever, does the server need to have authorized physical access? Obviously, the answer is Yes. However, if using the provisioned access language, the BCSI server physical access control would be ignored. The provisioned access to BCSI is not clear. When the BCSI is taken outside BCSI Repository, it is not practical for CIP-004 to manage the access to each piece of BCSI outside the BCSI repository. If a BCSI is under the personal control of the user who has authorized access to BCSI, it should be treated as BCSI access controlled and

should be addressed in CIP-011requirement for protecting and handling BCSI rather than in CIP-004. Also “authorized provisioned access to BCSI” has a wrong logical order since provisioning should happen after the authorization, but the wording can be interpreted to have authorization after provisioning.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The proposed language is too ambigious and obligates entities to protect BCSI in any form, even though beyond its control. Should BCSI be shared with NERC/FERC, the way CIP-004 reads in present state could be understood so as to require registered entities to extend their access management to be inclusive of a copy of that information held by NERC/FERC. And 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

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No
Document Name	

Comment

We do not see how the changes make any differentiation from Provisioning of physical access to BCSI and electronic access to BCSI. Was the thought that changing the Applicability wording from “BCSI associated with” to “BCSI pertaining to”, would provide the clarity that is being referenced? It is not clear where any clarity is provided.

Likes 1	Platte River Power Authority, 5, Archie Tyson

Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
The enforceable language in this version does not differentiate between physical and electronic access. If electronic BCSI is not stored or transmitted in a protected form, then physical access to electronic BCSI could permit the bypass of any electronic access controls.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
Part 6.3: We understand provisioned access to be a subset of access, and that access grants can be provisioned, inadvertent, or obtained in other ways. We think the intent of this Part is to remove all of the terminated individual's accesses to BCSI, not just provisioned access. The 'use' consideration is just perhaps misplaced within the sentence? Consider replacing "remove the individual's ability to use provisioned access to BCSI" with "remove the individual's ability to access and use BCSI".	
Likes 0	
Dislikes 0	
Response	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
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 this is an important distinction to make and the revision to CIP-004 clarifies this electronic/physical distinction with the deletion of R4.1.3. The revision does pose an issue as entities cannot prove the prevention of personnel seeing hardcopies (physical/printed) of network diagrams or other forms of BCSI. However, the Technical Rationale does explicity acknowledge that dilemma. For example, there is no available or feasible mechanism to provision access in instances when an individual is merely given, views, or might see BCSI, such as when the individual is handed a piece of paper during a meeting or views a whiteboard in a conference room. There will likely be no specific provisioning of access to BES Cyber System Information on work stations, laptops, flash drives, portable equipment, offices, vehicles, etc., especially when BCSI is only temporarily or incidentally located or stored there. That now deleted language was unclear at best if this distinction was even allowed. Removal of R4.1.3 has clarified that it is now possible to make this distinction. However, making this distinction is implied but never stated in R6.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	Yes
Document Name	

Comment

ATC appreciates the SDT's removal of BCSI from CIP-004-6 Requirements R4 and R5, and the result to keep this apart from the realm of physical access to where electronic BCSI may be physically stored, which has been a point of contention and confusion. Creating the new requirement R6 accomplishes this separation and clarity making it possible for the controls to not only be commensurate with risk, but also to be commensurate with the format of the BCSI and the types of methods available to protect digital vs hardcopy. This is very important in order to enable use of cloud-based solutions for CIP BCSI.

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3

Answer	Yes
Document Name	

Comment
BCSI requirements seem cleaner to be consolidated into R6, however the revisions have minimal impact to the provisioning aspects of the requirements. It has always been AEP's understanding that AEP is responsible the provisioning of physical access to physical BCSI and electronic access to electronic BCSI.

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
The concept of provisioned access to BCSI clarifies this, since provisioned access to a room where a physical server is housed does not in itself give access to the electronic BCSI on that server.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	

Comment
: PAC agrees with the revision. New language verifies provisioned access to BCSI is authorized and the provisioned access is appropriate based on need.

Likes 0	
Dislikes 0	

Response

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

Document Name	
Comment	
SRP agrees, but does not fully agree with the current wording.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Oncor supports EEI's 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	
Quintin Lee - Eversource Energy - 1	
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	
Kelsi Rigby - APS - Arizona Public Service Co. - 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	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	

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	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
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	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response
Carl Pineault - Hydro-Qu?bec Production - 5
Answer
Document Name
Comment
We support NPCC Regional Standards Committee 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
Document Name
Comment
Need to nail down “provisioning” in order to answer Yes or No Today’s technical access is the physical security provisioning. Prefer the intent of “provisioning” to be in the Measures instead of the Technical Guidance - - - possibly in Part 6.1 Removing the notion of access to designated storage locations, whether physical or electronic reduces any ambiguity it may have had with respect to the management of physical access where the BCSI resides on a electronic form. Emphasis could be placed on the concept introduced in the ERO Enterprise CMEP Practice Guide published on April 26, 2019 where access to the BCSI is defined by the individual ability to obtain and use the BCSI. Depending on the security measures in place (e.g. encryption with key management), it makes it explicit that an individual with physical access to a data center containing BCSI, but without the ability to use the BCSI (due to encryption) would not be within the scope of the requirement.

For exemple:

6.1 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

Ability to obtain and use BCSI, wheter physical or electronic.

6.2 Verify at least once every 15 calendar months that all individual's with ability **to obtain and use** BCSI:

6.2.1. Is authorized; and

6.2.2. Is appropriate based on need, as determined by the Responsible Entity.

6.3 For termination actions, remove the individual's ability to **obtain and use** 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.

If the intent was to make clarification about explicitly mentioning physical and electronic access, the SDT will need to make further revisions to clarify that.

Likes 0	
Dislikes 0	

Response

Becky Webb - Exelon - 6

Answer	
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	
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	
Document Name	

Comment

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

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

David Rivera - New York Power Authority - 3

Answer	
Document Name	

Comment

Need to nail down “provisioning” in order to answer Yes or No

Today’s technical access is the physical security provisioning. Prefer the intent of “provisioning” to be in the Measures instead of the Technical Guidance - - - possibly in Part 6.1	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,SERC,RF, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy needs more clarification on provisioning and managing as it applies to repositories versus discrete pieces of BCSI and electronic access to electronic BCSI.	
Likes 0	
Dislikes 0	
Response	

3. Do you agree the revisions to CIP-011 clarify the protections expected when utilizing third-party solutions (e.g., cloud services)?

Kjersti Drott - Tri-State G and T Association, Inc. - 1

Answer	No
Document Name	

Comment

Tri-State does not agree with the revisions.

We think 1.2 could cause audit approach confusion. In the measures would the expectation be we have identified data in a true data lifecycle methodology or just during use, transit, rest? We recommend the drafting team provide examples of what could be part of the data's lifecycle so it is clear what is intended (even though all states may not be applicable to every lifecycle).

As worded, a violation of R1.4 could also be considered a violation of R1.2. (double jeopardy) Instead, recommend combining R1.2 and R1.4 into one requirement. Additionally, recommend remove "for the separation of duties" from the measure as that could be interpreted in different ways and is not needed anyway to relay the intent.

Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

While the revisions add clarity for protections expected when utilizing third-party solutions such as cloud services for storage purposes, the "vendor services to utilize and analyze BCSI" lanuage presents a number of issues. R1.4 risk identification and assessment methods, as written, implies that this must be completed for all vendors that may have access to electronic of physical documentation containing BCSI. Vendors may only utilize information while onsite or may be authorized for access to BCSI for an engagement, but may never actually utilize or store this information. In these situations, the requirements to have to identiy and assess risks (R1.4) and then enforce at least one or more electonic technical controls (R1.5) are not value-added activities to the organization. To avoid scope creep, NERC may consider defining Vendor Services to define exactly what services are in scope.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10

Answer	No

Document Name	

Comment

Regarding usage of BCSI: We are unsure if the CIP-011-3 requirements that use the acronym “BCSI” are enforceable when the acronym is not included in the “BES Cyber System Information” NERC Glossary term. The acronym first appears in the purpose statement for CIP-011-3, but should the enforcement of the requirement depend on the purpose statement? Consider updating the "BES Cyber System Information" glossary term to include the new BCSI acronym as part of the CIP-011-3 draft. The acronym field for that glossary term is currently blank.

Part 1.3: The requirement in Part 1.3.1 doesn’t explicitly include data sovereignty, although the measures suggests that data sovereignty should be included. The omission of data sovereignty risk consideration in the requirement could represent an unaddressed risk for BCSI in a cloud service provider environment. Consider clarifying intent by aligning the language of the requirement with the language of the measure.

Part 1.3: We are unsure if risk management methods were intended for all vendor services related to BCSI, or just for the storage, utilize, or analyze cases. Consider changing “storage, utilize, or analyze, to “… including but not limited to storage, utilize, or analyze BCSI…” to ensure that all vendor services related to BCSI are covered.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

CIP-011-3 R1 Part 1.3 uses these terms without an accompanying definition: Data governance, rights management, identity management, access management, security management, application security, infrastructure security, and network security. Some examples are given in the Measures, but clear definitions, or referenced to documents that provide definitions, should be included.

Part 1.3 also groups different concepts into a single sub-part. Consider separating single sub-parts into definied and catergorized separate sub-parts. For example, 1.3.4 Application security; 1.3.5 Infrastructure security; and 1.3.6 Network security.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No

Document Name	

Comment

Having “Data Governance” listed under 1.3 risk management methods seems out of place and maybe duplicative. The measurement for 1.3.1 also seems to imply requirements that are not in the requirement column. The requirements seem broad and the measures are less clear and seem to add to the requirements. How does requirement 1.3.3 “Security management” differ from “Application, infrastructure and network security.” Should some of these requirements fall into CIP-013 when contracts are established for services?

Consider remove Data Governance from the requirement.

Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

TVA does not believe that the CIP-011 Requirements R1.3 and R1.4 are needed. CIP-011 R1.3 is within scope of CIP-013 service procurement and should be addressed as part of that assessment. R1.4 protections mechanisms are covered in CIP-011 R1.2 and do not need to be duplicated in R1.4. R1.2 does not put limits on the scope of the mechanisms, and applies to the BCSI in all cases durings its lifecycle. We recommend adding the clause in the measures first bullet point, *Evidence of methods used to protect and securely handle BCSI during its lifecycle, by any authorized party or individual, including:*. We believe inclusion of this statement will clarify that the scope of the protection methods established are inclusive of the environments, transmission, and any interactions with the information.

Under Requirement 1.1 the changes to the standard moves the protection to the BCSI itself rather than the repositories that housing it. The last measure, which identifies storage locations, should be removed or modified to allow the entity to demonstrate the data flow of BCSI from the source BCS after identification. The language as proposed would make every BCA a BCSI storage location.

In requirements R2.1 and R2.2, the scope should be limited to Cyber Assets that contain accessible BCSI.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

SRP agrees with the overall direction and what this version is trying to accomplish. We struggle with the four sub requirements in R1.3. We believe there is overlap and potential confusion in terms. For example, isn't "identity and access management" and "network security" a part of "security management"? The term "security management" is too broad. How is "rights management" different than "identity and access management"?

Also, when putting the R1.3 Requirement into individual sentences, they read:

- Implement risk management method(s) for **Data governance and rights management**
- Implement risk management method(s) for **Identity and access management**
- Implement risk management method(s) for **Security management**
- Implement risk management method(s) for **Application, infrastructure and network security**.

SRP suggests removing each of them from unique subrequirements.

Also, our concern is the wording provides too much flexibility in determining methods and defining the four topics. This will result in a wide range of methods implemented. We fear as written this requirement will create unintended consequences and become as difficult to interpret and implement as CIP-013 has been for the industry.

The technical rationale on the bottom of page 2 states "Implemented identification and assessment methods are needed to understand the risks to BCSI when choosing to use vendor services." This statement is more clear on what to do for R1.3 than what is written in the proposed requirement. Consider verbiage like this without subrequirements.

R1.3 and R1.4 read different than R1.1 and R1.2. R1.1 and R1.2 start with "Method" and R1.3 and R1.4 start with an applicability statement. The applicability statement should be in the applicability column.

Consider updating the Applicability in R1.3 and R1.4 to:

"**BCSI as identified in Part 1.1 when the Responsible Entity engages vendor services to store, utilize, or analyze BCSI**"

Then the R1.3 requirement can read:

"Implement one or more processes for identifying the risk of using vendor services to store, utilize, or analyze BCSI"

Then the R1.4 requirement can read:

"Implement one or more documented electronic technical mechanisms to protect BCSI when using vendor services to store, utilize, or analyze BCSI"

Overall, we need better clarification on how this is the same or different than CIP-013.

Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	

Comment
Part 1.3 should belong to CIP-013 since it is a vendor risk assessment item. Using requirement CIP-004 Part 6.1.4 we suggest in question 1, CIP-011 Part 1.4 should be moved to the Measures of CIP-004 Part 6.1.4 on how to control the access to the BCSI repository. CIP-011 requirements like other CIP-004 requirements should apply to the responsible entities as well as vendors by default and don't need to define vendor only requirements in CIP-11. The current version of CIP-011, vendor requirements are described in Guidelines and Technical Basis.

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	No
Document Name	

Comment
Puget Sound Energy supports the comments of EEI.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3	
Answer	No
Document Name	

Comment
Recommend a change to Part 1.4's requirement to explicitly say "electronically." Change from When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI. To When the Responsible Entity engages vendor services to electronically store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI. Alternatively the Applicability column could specify "electronic."

Likes 0	
Dislikes 0	

Response

Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo

Answer	No
Document Name	

Comment

The proposed R1.3 does not state any security controls that need to be implemented. The proposed R1.3 essentially requires entities to have a framework to manage risks associated with utilizing third party for storing, utilizing or analyzing. The proposed risk management framework needs to be implemented for 1.3.1 to 1.3.4.

We also believe that the term “utilize” in the proposed R1.3 is too broad. Requirements should focus on storage and analysis only.

While we welcome this approach since a one solution fits all may not exist; however, practicality of implementing such a framework is not clear. Perhaps, similar language to CIP-013 may be needed (risk-based approach) and use of terms such as the “the risk management methods need to address”.

The proposed R1.4 no longer suggests that protection at BCSI level (encryption) is a must. Instead, CIP-011 R1 will require a mechanism to protect BCSI. We still believe that protection must be applied at the BCSI level when stored/analyzed on a third party cloud.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

The SAR is focused on cloud service providers, but the requirement potentially pulls in many other vendor services, such as engineering consultants who may occasionally be provided temporary access to a document that is considered BCSI. Clarification in the standard language or applicability should address the intended scope.

CIP-013 doesn’t require audits of vendor performance and adherence, where CIP-011 without similar exception would require these types of verifications for compliance. This is beyond the scope of the NERC CIP Standards to audit external third parties that are not Registered Entities compliance to the requirements.

Likes 0	

Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
While the sub-parts of CIP-011-2 R1.3 appear to *imply* protections are only for electronic BCSI stored by vendor services. The language of the standard does not explicitly make this distinction. The language should be clarified accordingly to avoid confusion pertaining to physical BCSI for which vendor services may be engaged to store, utilize, or analyze BCSI.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
The SAR references “third party storage and analysis” but the requirement refers to “vendor services to store, utilize or analyze BCSI.” The SAR is focused on cloud service providers, but the requirement potentially pulls in many other vendor services, such as engineering consultants who may occasionally be provided a drawing that is considered BCSI. Change the text to be consistent with the SAR: “third party storage and analysis.” Consider limiting the scope to “data hosting” vendor services. If it was the standard drafting team’s intent to exclude temporary use of BCSI, it should be addressed in the technical rationale or requirement text. Also, there is nothing in the technical rationale excluding other entities and regulators from being considered “vendors.” CIP-013-1 R2 includes language that should be considered for CIP-011 R1.2: vendor performance and adherence to a contract are beyond the scope of the requirement. Remove the prescriptive sub parts on 1.3 and make the requirement simply: implement risk management methods. Allow the Registered Entities the flexibility to determine the appropriate components of risk management. Also, limit the requirements to match the applicability of CIP-004-6 R6. This should not be required for medium impact without ERC. To improve clarity, repeat the applicability on each subpart, rather than referring back to an earlier subpart.	
Likes 0	
Dislikes 0	
Response	

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

The SAR references “third party storage and analysis” but the requirement refers to “vendor services to store, utilize or analyze BCSI.” The SAR is focused on cloud service providers, but the requirement potentially pulls in many other vendor services, such as engineering consultants who may occasionally be provided a drawing that is considered BCSI.

Change the text to be consistent with the SAR: “third party storage and analysis.” Consider limiting the scope to “data hosting” vendor services. If it was the standard drafting team’s intent to exclude temporary use of BCSI, it should be addressed in the technical rationale or requirement text. Also, there is nothing in the technical rationale excluding other entities and regulators from being considered “vendors.”

CIP-013-1 R2 includes language that should be considered for CIP-011 R1.2: vendor performance and adherence to a contract are beyond the scope of the requirement.

Remove the prescriptive sub parts on 1.3 and make the requirement simply: implement risk management methods. Allow the Registered Entities the flexibility to determine the appropriate components of risk management.

Also, limit the requirements to match the applicability of CIP-004-6 R6. This should not be required for medium impact without ERC. To improve clarity, repeat the applicability on each subpart, rather than referring back to an earlier subpart.

Likes 0	
Dislikes 0	
Response	

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	

CEHE agrees that the CIP-011 Requirement R1, Parts 1.3 and 1.4 clarify the protections expected when using third-party cloud services. However the requirement has much broader language that could be problematic. First, the term “Vendor services” goes beyond cloud services and could create unintended issues for other types of vendor services. Second, use of the term “BCSI” can imply both physical and electronic BCSI, which may cause a

problem because sub-part 1.3.4 would not apply to physical BCSI. Additionally, Part 1.4 that requires an entity to "implement documented electronic technical mechanisms" could not be applied to physical BCSI.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5, Group Name NCPA

Answer	No
Document Name	

Comment

See Tristate (SAR originator) and SMUDs comments.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

PG&E believes the modifications to clarify that third party solutions can be used, but the Requirement language in Parts 1.3 and 1.4 are vague. PG&E understands the vagueness is necessary to allow for the many possible methods of protecting BCSI with a third-party. PG&E believes the Measures and Technical Rational (TR) document provide sufficient information to allow an Entity to adequately protect their BCSI, but the Measures and TR are not the Standard which could lead to interpretation differences between an Entity and Audit Team. PG&E does not have a suggestion at this time to improve the vagueness but is willing to work with the SDT and industry to address this concern.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment
DOminion Energy supports the comments by EEI and agrees for the need to replace or clarify the term vendor services with a more narrowly and clearly defined term. There should be a clear deliniation between services that are off-premise and those that are housed on infrastructure directly controlled by the entity.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	

Comment
Regarding CIP-011-3 R1 Part 1.3, the terminology for the sub-parts do not add value to CIP-011. It is unclear what this terminology would require or what any of these terms mean, making them subject to broad and differing interpretation. The risk, which is unauthorized access, is currently being addressed by an entity's approach to satisfying CIP-011 part 1.2 and CIP-004 R6. What is the justification for this language if protection and access management is already required? The phrase "implement risk management" is unclear and open to interpretation. This proposed requirement is a paperwork exercise that adds administrative burden without realizing security benefits. Auditability will be difficult and open to interpretation. For these reasons, MPC proposes striking this requirement and relying on access management in CIP-004 and CIP-011 part 1.2 for protection of BCSI. For R1, parts 1.3 and 1.4, the phrase "engages vendor services to store, utilize, or analyze BCSI" does not clarify when or where this requirement is applicable. This could apply to an onsite vendor or contractor, when it seems this requirement is intended to address cloud service providers. MPC requests SDT consideration of alternative phrasing for 1.3, if CIP-011 part 1.3 is not struck as requested above, and 1.4 such as: "…service provider on service provider-owned or -managed premises or computing infrastructure…"

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3	
Answer	No
Document Name	

Comment
'Utilizing' leaves room for guessing. Why not consistently say – "transit, storage and use" like everywhere else in the document? AEP is also concerned with any unintended consequences from the proposed language, as it could be interepted to mean any vendor's use of BSCI, even if it is stored on AEP's systems, and not BSCI that is stored, transmited, or used by a 3rd party vendors on their system(s).

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 believes proposed Requirement R1 Part 1.3 has two significant problems. The first is that it seems to have been developed with vendor risk management in mind. If so, N&ST believes requirements to evaluate the risks associated with allowing any particular vendor to "store, utilize, or analyze" BCSI should be added to CIP-013, not CIP-011. The second is that in N&ST's opinion, the language of sub-parts 1.3.1 through 1.3.4, (e.g., 1.3.1, "Data governance and rights management") is vague to the point of lacking any intrinsic meaning. Furthermore, while we generally don't comment on proposed Measures, we are at a loss to understand what the example, "Vendor certification(s) or Registered Entity verification of vendor controls implemented from the under-layer to the service provider, including application, infrastructure, and network security control s as well as physical access controls" is intended to mean.

N&ST is also concerned about proposed Requirement R1 Part 1.4. While we agree it is a good security practice to "implement one or more documented electronic technical mechanisms to protect BCSI," we note the proposed requirement, as written, appears to apply only to situations where "the Responsible Entity engages vendor services to store, utilize, or analyze BCSI."

Finally N&ST notes that the latest revisions appear to have removed the requirement to protect BCSI (against, we presume, unauthorized disclosure), while "in transit." N&ST assumes this was unintentional.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Oklahoma Gas & Electric supports the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

We support NPCC comments:

Recommend a change to Part 1.4's requirement to explicitly say "electronically."

Change from

When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.

To

When the Responsible Entity engages vendor services to electronically store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.

Alternatively the Applicability column could specify "electronic."

Likes 0	
Dislikes 0	
Response	

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	

We agree that the revisions clarify the protections expected to be compliant, however, if it is the SDT's intent to have a risk assessment performed for 3rd party storage systems, then those requirements should be a part of CIP-013. This is not in the scope of the SAR, but should have been considered.

Secondly, requirements R1.3.1-1.3.4, are very dynamic for the majority of major Cloud Service Providers (CSP) and would require periodic/continuous risk assessments due to the nature of 3rd party storage services. As a 3rd party storage service customer, you are at the mercy of the CSP's terms and conditions, features, security features, IAM, encryption, etc. which may change at any time causing a change in risks. A change in terms and conditions, security features, IAM, purchasing additional security features, etc. would trigger a new risk assessment that would make compliance onerous.

Also, the configuration (hybrid, private, public) of cloud/3rd party services, severely impacts the potential threats to the unauthorized access to BCSI which is not considered in the requirements. For major CSPs as a 3rd party storage solution provider in a private configuration is no different than the BCSI being stored on premise.

Lastly, the way the question is being asked using “third-party solutions” (e.g. cloud services) instead of the language used in the requirements makes it difficult to answer without making assumptions.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

ATC appreciates the use of the word “vendor” instead of “third party” to assure clarity that this refers to an entity that is not a Registered Entity. That having been said, the proposed words in CIP-011=3 might not go far enough on two points.

1. The words in CIP-011-3 Requirement R1 Parts 1.3 and 1.4 do not accomplish the level of specificity needed to assure the scope is appropriately limited to cloud type, off-premises solutions/services owned and managed by an entity that is **not** a Registered Entity. Unfortunately, the words as currently proposed carry the unintended consequence that a Registered Entity would have to perform a risk assessment on their own on-premises infrastructure. Additionally, to enable use of cloud-based solutions for BCSI while maintaining an objective, risk-based, and technology/platform agnostic requirement is equally important

2. In the current proposed draft, the use of the defined term BCSI without a scoping adjective of “electronic” or “digital” preceding it in these requirements continues to breed confusion that physical methods may also be needed; creating misalignment with the SAR’s intent is to enable use of electronic controls as the methods to protect BCSI where off-premises cloud-based solutions are used. The existing CMEP Practice Guide makes a concerted effort to separate physical controls for physical BCSI from electronic controls for electronic BSCI, bringing great clarity to the fact that electronic controls can be as secure, if not potentially more secure for electronic format BCSI than the physical controls like a PSP. This requirement language must achieve that same level of clarity to enable these requirements for cloud to actually be implemented without any misunderstanding that physical controls also must apply.

For these reasons, ATC requests SDT consideration alternative phrasing like this.

CIP-011-3 Requirement R1 Parts 1.3

1.3 For storage, utilization, or analysis of electronic BSCI performed by a service provider on service provider-owned or -managed premises or computing infrastructure, implement risk management method(s) for the following:

1.3.1 Data governance and rights management; and

1.3.2 Identity and access management; and

1.3.3 Security management; and

1.3.4 Application, infrastructure, and network security.

CIP-011-3 Requirement R1 Parts 1.4

1.4 For storage, utilization, or analysis of electronic BSCI performed by a service provider on service provider-owned or -managed premises or computing infrastructure, implement one or more documented electronic technical mechanisms to protect BCSI.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

GSOC greatly appreciates the SDT's consideration of its previous comments regarding the retention of all BCSI program requirements in CIP-011. However, it does not support the revisions to CIP-011 to clarify the protections expected when utilizing third-party solutions (e.g., cloud services) – as proposed – and provides the following comments for the SDT's consideration:

1. **Modification of Established Format** - As stated in its previous comments, while GSOC understands what the SDT was attempting to accomplish, it does not agree with the replacement of "Applicable Systems" with "Applicability." "Applicability" is already utilized in each of the reliability standards to denote whether or not a particular registered function has responsibility under the Standard. Utilization of the same term, but with a different scope of applicability within body of CIP-011 will result in confusion and ambiguity regarding the overall applicability of this reliability standard. Further, this change results in this Standard and CIP-004 (where this change has also been proposed) being different from the remaining CIP reliability standards relative to the CIP reliability standards overall approach to identification of asset scope. GSOC raises, for the SDT's consideration, that the deviation from the established format and scoping mechanisms used throughout the CIP reliability standard will create confusion and ambiguity and that any value achieved by this change will be far outweighed by the continued value associated with the current format and terms.

To address this concern, GSOC proposes that the lead in requirement language for requirement R6 be modified as follows:

Each Responsible Entity shall implement one or more documented information protection program(s) for BES Cyber System Information about the "Applicable Systems" identified in CIP-0011-3 Table R1 – Information Protection Program that collectively include each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].

2. Potential Scope Expansion - GSOC notes that it is also concerned that the modifications to the contents of the "Applicability" column may potentially expand and obscure the established definition of BCSI set forth in the Glossary of Terms Used in NERC Reliability Standards. First, GSOC notes that the Applicability columns proposed between CIP-004 and CIP-011 are different. In particular, CIP-004 utilizes the terms "BCSI associated with …" while CIP-011 utilizes the terms "BCSI pertaining to…" BCSI is defined as

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

Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

The use of the term "pertaining to…" is similarly subjective to the term "associated with" and could, therefore, also be interpreted broadly by some entities and/or regulators. As an example, information about an external firewall configuration that acts as a first line of defense, but is not part of an applicable system, may contain information that "could be used to gain unauthorized access or pose a security threat to the BES Cyber System." It is unclear under the proposed revisions to the applicability column whether this information would be considered subject to CIP-004 – even if the asset from which it came is not in scope for any other reliability standards. Moreover, these new terms as proposed in CIP-011 and CIP-004, although similar, could be interpreted differently between these two related standards, between Responsible Entities, and between Responsible Entities and Regulators. Such differing interpretations could result in both compliance and security-related concerns.

Finally, this potential scope expansion, conflict, and the associated ambiguity between the scope of CIP-004, CIP-011, the remaining reliability standards, and the Glossary of Terms Used in NERC Reliability Standards could result in increased compliance obligations without an attendant security or reliability benefit, confusion, and inconsistency of implementation. The proposed revision above would resolve this issue by eliminating the differing terms, while preserving the current format of CIP-011 and its consistency with the remaining reliability standards.

3. Backwards compatibility – GSOC is concerned that the proposed revisions for requirements R1.1 and R1.2 may not be compatible with Responsible Entities' existing programs. More specifically, many current programs have been developed and are managed around the concept of repositories or storage locations – not individual pieces of BCSI. The modifications of requirements R1.1and R1.2 (when coupled with the revisions to the Applicability Column) appear to shift focus to each individual piece of information – without flexibility to identify information based on their repository or storage location.

For this reason, GSOC respectfully suggests that the proposed requirements are not backwards compatible and would require significant effort to implement. This is because the obvious implementation method to ensure compliance would be to create and maintain a list of each individual piece of BCSI, its location, and its format. Such a list would be a new development that would likely not be compatible with existing program implementations. To address these concerns, GSOC recommends rewording requirement R1.1 as follows:

Method(s) to identify BCSI or their storage locations/repositories, as applicable

This would allow entities the flexibility to manage BCSI based on the most secure approach to such management, e.g., by repository or by pieces of information as it applies to their environment.

4. Ambiguity – GSOC is concerned that a number of the proposed revisions introduce ambiguity that could lead to differing interpretations and implementation for requirements R1.2 – R1.4. Relative to requirement R1.2, GSOC respectfully suggests that, contrary to the Technical Rationale, the removal of state references from the requirement and their replacement with more generic terms increases confusion and does not make the obligations more "explicitly comprehensive." In particular, GSOC notes that the previous state references (use, storage, transit, etc.) were well known and well understood concepts. Their replacement with a generic requirement to "protect and securely handle" could result in various interpretations and implementation of those obligations. Moreover, it could result in a security-related deficiency should an entity construe such terms narrowly.

Additionally, relative to requirements R1.3 and R1.4, GSOC is concerned that the term "vendor solutions" could be interpreted broadly to include "on-premises" vendor solutions that are managed by the responsible entity. For example, if an entity purchases and hosts "on prem" a document management system provided by a vendor, e.g., IBM, Microsoft, etc., would that "vendor solution" be subject to CIP-011, requirements R1.3 and R1.4. It is unclear from the language contained in the proposed revisions or the Technical Rationale what comprises or meets the definition of "vendor services." Accordingly, this term is open to interpretation and could lead to an overall scope expansion for this small subset of requirements – as unintended as that scope increase may be. Moreover, such scope expansion may increase Responsible Entity's obligations without an attendant increase in overall security or reliability – especially where additional requirements are applied to "on prem" "vendor solutions" that are managed by responsible Entities.

Further, GSOC notes that the terms introduced in requirement R1.4 may not all be well understood across the industry and should not be introduced without definitions or other guidance. As an example, the term "data governance" is not a well understood term across the industry and is not defined in these proposed revisions. Introducing this term and its associated "rights management" without any scope, context, or definition that would elucidate what it means in this use would be problematic as it has a high potential for confusion, ambiguity, and subjective interpretation. Moreover, as applied to potential "vendor solutions" (whether on- or off-premises), requirements R1.3 and R1.4 may be duplicative of each other and may be duplicative of what

is required in CIP-004 as well as other reliability standards. At a minimum, GSOC recommends combining requirements R1.3 and R1.4 and better defining those instances to which they apply.

5. Unintended consequences - GSOC is concerned that the proposed revisions to CIP-011 and CIP-004 result in significant program modifications and additional obligations for Responsible Entities regardless of whether they are using any cloud services, and, further, without modifications, vendors who have not engaged any cloud services and have not, therefore, modified their BCSI programs could be found non-compliant with these revised requirements. It respectfully asserts that requiring Responsible Entities that are not engaging in cloud-based services to overhaul their entire information program to support others who want to migrate to the cloud is manifestly unfair, unduly burdensome and a risk to reliability.

The placement of new and unnecessary compliance obligations and the potential expansion of the scope of CIP-011 for those entities that have chosen not to engage in the storage, handling, or use of BCSI in a cloud has the potential to divert resources to the implementation of new and different program aspects. Such diversion increases the risk of a deficiency or failure for issues that would be better addressed in implementation or compliance guidance. For these reasons, GSOC is concerned that the proposed revisions are not properly scoped to ensure compatibility with existing programs while accommodating the evolving storage and other solutions that could be employed in the future.

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	No
Document Name	

Comment

SDG&E supports EEI's comments submitted on our behalf.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO-NSRF comments.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
See Tristate (SAR originator) and SMUDs comments.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
The SAR is focused on cloud service providers, but the requirement potentially pulls in many other vendor services, such as engineering consultants who may occasionally be provided temporary access to a document that is considered BCSI. Clarification in the standard language or applicability should address the intended scope. CIP-013 doesn't require audits of vendor performance and adherence, where CIP-011 without similar exception would require these types of verifications for compliance. This is beyond the scope of the NERC CIP Standards to audit external third parties that are not Registered Entities compliance to the requirements.	
Likes 0	
Dislikes 0	
Response	
Larry Snow - Cogentrix Energy Power Management, LLC - 4 - NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
R1.4 should specify "electronically store".	
Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The IRC SRC recommends a change to Part 1.3's requirement as detailed below. Recommend any additional detail needed to describe risk management methods be captured under CIP-013.

When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement risk management method(s).

Recommend a change to Part 1.4's requirement to explicitly say "electronically" as detiled below:

When the Responsible Entity engages vendor services to ***electronically*** store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.

Alternatively the Applicability column could specify "electronic."

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	No
Document Name	

Comment

Recommend a change to Part 1.4's requirement to explicitly say "electronically."

Change from

When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.

To

When the Responsible Entity engages vendor services to electronically store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.

Alternatively the Applicability column could specify "electronic."

The proposed R1.3 does not state any security controls that need to be implemented. The proposed R1.3 essentially requires entities to have a framework to manage risks associated with utilizing third party for storing, utilizing or analyzing. The proposed risk management framework needs to be implemented for 1.3.1 to 1.3.4.

We also believe that the term "utilize" in the proposed R1.3 is too broad. Requirements should focus on storage and analysis only.

While we welcome this approach since a one solution fits all may not exist; however, practicality of implementing such a framework is not clear. Perhaps, similar language to CIP-013 may be needed (risk-based approach) and use of terms such as the "the risk management methods need to address".

The proposed R1.4 no longer suggests that protection at BCSI level (encryption) is a must. Instead, CIP-011 R1 will require a mechanism to protect BCSI. We still believe that protection must be applied at the BCSI level when stored/analyzed on a third party cloud.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

EEI recognizes SDT efforts to clarify the protection expectations needed by entities when utilizing third-party solutions but suggests the following changes to better clarify the needed protections:

Requirement 1

Part 1.2 Measures

1. EEI suggests modifying Bullet 2 to begin with the phrase "evidence demonstrating" to further clarify the Measure
2. EEI suggests adding the following measure: A documented process for protecting and securely handling BCSI.

Part 1.3 & 1.4: "Vendor services" is an overly broad term that is not limited to cloud services, and when combined it with the phrase "to utilize or analyze BCSI", brings in additional scenarios, such as engaging a vendor service on-premise at the Responsible Entity's location with the Responsible Entity's equipment to analyze BCSI (for example, in an incident response/forensics situation). Additionally, the requirement language does not link vendor services to BCSI that is stored, used, or analyzed off-premise on a vendor's infrastructure. "Engaging a vendor service" encompasses more than a cloud service offering and the resulting 1.3.1-1.3.4 methods are not applicable to a vendor providing services on site using the entity's own equipment. Both 1.3 and 1.4 begin with "When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement …." We suggest changing both to clarify cloud-based scenarios such as "When the Responsible Entity engages ***off-premise*** vendor services to store, utilize, or analyze BCSI, implement…" or possibly "When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI ***on the vendor's infrastructure***, implement…"

Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
While the revisions do clarify the protections expected when utilizing third-party solutions, the revisions do not have a narrowed scope. BCSI may be shared with mock auditors who will be analyzing BCSI. More clarity is required on the measures to determine the intended scope of the requirement changes. Unclear if these requirements are retroactive to contracted vendors or if these will apply to only new vendors.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
Please elaborate on what is required for CIP-011 R1.3.1 Data Governance and Rights Management.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
We support NPCC Regional Standards Committee comments	
Likes 0	

Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	

Comment
CAISO is in support of the below IRC SRC comments: The IRC SRC recommends a change to Part 1.3's requirement as detailed below. Recommend any additional detail needed to describe risk management methods be captured under CIP-013. When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement risk management method(s). <To remove the below: "for the following: 1.3.1 Data governance and rights management; and 1.3.2 Identity and access management; and 1.3.3 Security management; and 1.3.4 Application, infrastructure, and network security.">> Recommend a change to Part 1.4's requirement to explicitly say "electronically" as detiled below: When the Responsible Entity engages vendor services to electronically store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI. Alternatively the Applicability column could specify "electronic."

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

We agree that the revisions clarify the protections expected to be compliant, however, if it is the SDT's intent to have a risk assessment performed for 3rd party storage systems, then those requirements should be a part of CIP-013. This is not in the scope of the SAR, but should have been considered.

Secondly, requirements R1.3.1-1.3.4, are very dynamic for the majority of major Cloud Service Providers (CSP) and would require periodic/continuous risk assessments due to the nature of 3rd party storage services. As a 3rd party storage service customer, you are at the mercy of the CSP's terms and conditions, features, security features, IAM, encryption, etc. which may change at any time causing a change in risks. A change in terms and conditions, security features, IAM, purchasing additional security features, etc. would trigger a new risk assessment that would make compliance onerous.

Also, the configuration (hybrid, private, public) of cloud/3rd party services, severely impacts the potential threats to the unauthorized access to BCSI which is not considered in the requirements. For major CSPs as a 3rd party storage solution provider in a private configuration is no different than the BCSI being stored on premise.

Lastly, the way the question is being asked using "third-party solutions" (e.g. cloud services) instead of the language used in the requirements makes it difficult to answer without making assumptions.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Southern does not agree that CIP-011 clarifies the protections expected when utilizing third-party solutions. Per the TR, the different states of information from the requirement have been removed. "By removing this language, methods to protect BCSI becomes explicitly comprehensive." The SDT needs to clarify exactly what that means. Removing the language now seems to cause more confusion where this was intended to address.

The methods in requirement **R1.2** state to "protect" and "securely handle" BCSI. The two seem to be synonomous with each other and have no difference. Suggested restatement to simply use "securely handle" which has greater clarity and is sufficient on its own. The final bullet within the measures reads as a statement rather than an example of evidence as well as restates the information listed in the first bullet and should be changed to be an example of evidence different than the first bullet, or removed altogether.

R1.3 "Vendor services" is an overly broad term that is not limited to cloud services. When combined with "to utilize or analyze BCSI", it now includes numerous scenarios such as engaging a vendor service on-premise at the Responsible Entity's location with the Responsible Entity's equipment to analyze BCSI (example: a computer forensics company on retainer that is brought in to analyze an incident with a BCS). There is nothing in the requirement language that scopes it to BCSI that is stored, used, or analyzed off-premise on the vendor's infrastructure. "Engaging a vendor service" encompasses much more than a cloud service offering and the resulting 1.3.1-1.3.4 methods are not applicable to a vendor providing services on site using the entity's own equipment.

R1.3.3 (Security management) is a superset of the other three areas. 1.3.1 covers security of the data, 1.3.2 covers security of people, 1.3.4 covers security of the technology so 1.3.3 seems duplicative unless the intent is '*physical* security management' and if that is the intent, we suggest making that explicit.

The second bullet under Measures states that a list of risk assessment methods is "per vendor". We suggest striking this bullet as its covered by the first bullet and entities may have one risk management method that applies to all vendors, not per vendor.

R1.4 has the objective of simply "protect BCSI" but does not clarify "protect from what." The last bullet point under the Measure implies we are to protect the BCSI from subversion of the entity's control(s) by the custodial vendor. If that is the objective, we suggest that be placed in the requirement language for clarity as to the objective. Without further clarity, R1.4 is simply one scenario of R1.2.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

ITC supports the Comment Form submitted by EEI

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Agree with EEI's comments regarding confusion around "vendor services." If the SDT's intent is not to include BCSI in transit or for vendor services not storing but utilizing and analyzing BCSI for a short term/temporary engagement, that should be made clearer.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Bryan Taggart, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Grant Wilkerson, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Co, Evergy companies, incorporate by reference Edison Electric Institute's response to Question 3.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 5,6

Answer	Yes
Document Name	

Comment

The expectations regarding the utilization of third-party services seem clearer in this draft. However, with respect to CIP-011, specifically R1.4, it is apparent that a full security assessment will need to be performed on the vendor(s) in order to ensure compliance with the standard. As such, it would be helpful if the “Measures” section referenced specific acceptable standard certifications, such as SSAE 18 or FedRAMP. It should also be noted that vendors do not typically provide their security plan, when requested. This may make holistic security assessments difficult to complete.

Likes 0	

Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
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	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
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	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
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	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
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	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,SERC,RF, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy needs more clarification on what constitutes “engaging in vendor services” versus need to know sharing of a limited piece of BCSI with a third-party consultant.	
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	

Kinte Whitehead - Exelon - 3	
Answer	
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	
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	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

4. Do you agree the new and revised VSL/VRF descriptions clearly align with the revisions to CIP-004 and CIP-011?

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

We do not agree with the VSL/VRF because of our answer in question #3 above.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

CAISO is in support of the below IRC SRC Comments:

Within CIP-004: Changes were with R4, R5 and new R6.

Within CIP-011: Request clarification that violating more than two of the sub-requirements (ex. Part 1.3), not the items beneath 1.3

Request clarification that violating more than two of the sub-requirements (ex. Part 1.3) counts as just Part 1.3 or a failure at the R1 level.

Earlier version of CIP-011 appeared to be more Pass/Fail. This version has gotten much more granular in its description and implementation in sub-requirements. The auditing has generally occurred at the highest level (ex. Level 1 not Level 1.1, 1.2, 1.3). With the greater detail in the sub-requirements, flexibility decreases and the administrative burden required to demonstrate compliance increases without commensurate security benefits. If a Responsible Entity failed on one of the (new) sub-requirements, the violation is still rolled out at the R1 level. In looking through the VSLs, the changes between Lower and Severe amplify in relation to the number of sub-requirements missed as opposed to how many times the overall requirement was missed.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment	
We support NPCC Regional Standards Committee 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	No
Document Name	
Comment	
Request clarification that violating is at the CIP-004 Part level (6.2) not the items beneath Part 6.2 Request clarification that violating is at the CIP-011 Part level (1.3) not the items beneath Part 1.3	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management	
Answer	No
Document Name	
Comment	
Within CIP-004: Changes were with R4, R5 and new R6. Within CIP-011: Request clarification that violating more than two of the sub-requirements (ex. Part 1.3), not the items beneath 1.3 Request clarification that violating more than two of the sub-requirements (ex. Part 1.3) counts as just Part 1.3 or a failure at the R1 level. Earlier version of CIP-011 appeared to be more Pass/Fail. This version has gotten much more granular in its description and implementation in sub-requirements. The auditing has generally occurred at the highest level (ex. Level 1 not Level 1.1, 1.2, 1.3). With the greater detail in the sub-requirements, flexibility decreases and the administrative burden required to demonstrate compliance increases without commensurate security benefits. If a Responsible Entity failed on one of the (new) sub-requirements, the violation is still rolled out at the R1 level. In looking through the VSLs, the changes between Lower and Severe amplify in relation to the number of sub-requirements missed as opposed to how many times the overall requirement was missed.	

Likes 0	
Dislikes 0	
Response	
Larry Snow - Cogentrix Energy Power Management, LLC - 4 - NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
Better clarification is needed as to which items fall into the violations versus the items below CIP-004 Part 6.2 and CIP-011 Part 1.3	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
The proposed VSLs/VRFs align with the proposed revisions for CIP-004 and CIP-011.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
We do not agree with the VSL/VRF because of our answer in question #3 above.	
Likes 0	

Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
We support NPCC comments: Request clarification that violating is at the CIP-004 Part level (6.2) not the items beneath Part 6.2 Request clarification that violating is at the CIP-011 Part level (1.3) not the items beneath Part 1.3	
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 response to this question is based on our objections to the proposed revisions to CIP-004 and CIP-011.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3	
Answer	No
Document Name	

Comment
AEP believes that with the possible extension of BCSI to cloud providers, and the fact that there have been significantly more sophisticated, and a greater volume of, attacks against the energy industry, especially through phishing, that the VRF for R1 should be High. Additionally, with known foreign ownership, control, or involvement in PC reclamation and recycling, and the focus of foreign adversaries trying to gain access, cause damage, or control the US Power grid, the VRF for R2 should also be High. We agree with the VSLs as written, but believe the VRFs should be changed. Also, CIP-004-6 VSL/VRF is provided at requirement subpart level, while the revisions summarize at requirement level. Expanding to make CIP-004 R6 to indicate VSL/VRF at requirement subpart level might be more helpful.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3	
Answer	No
Document Name	

Comment
Request clarification that violating is at the CIP-004 Part level (6.2) not the items beneath Part 6.2 Request clarification that violating is at the CIP-011 Part level (1.3) not the items beneath Part 1.3

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	No
Document Name	

Comment
Puget Sound Energy supports the comments of EEI.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
Suggest adding a lower VSL to CIP-011 R2 for not having a documented process, and a High VSL for not following the documented process and releasing or disposing of a BCA with accessible BCSI. The enforcement of R2 is not the same as the enforcement of R1.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
The VSLs for CIP-004-7 R6 and CIP-011-3 R1 do not adequately reflect the severity of a possible violation. For example, failure to properly identify BCSI could result in a high reliability risk. But since this would only be a violation of one part of CIP-011-3 R1 the VSL assigned would be “Lower.” This does not adequately assess the severity of the violation. This is especially true of CIP-011-3 R1 where Parts 1.2, 1.3 and 1.4 apply to BCSI as identified in Part 1.1.	
Likes 0	
Dislikes 0	
Response	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	

Answer	No
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	Yes
Document Name	
Comment	
ITC supports the Comment Form submitted 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 the revisions to VSL/VRF for CIP-004 and CIP-011 are aligned properly based on the revisions in the respected Standards and Requirements.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	

Comment	
NVE supports the new and revised VSL/VRF descriptions	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
SDG&E supports EEI's comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E has no comments on the revised VSL/VRF's.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	

PAC agrees with the new and revised VSL/VFR desciptions.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees the VSL/VRF matrix reflects accurately.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Bryan Taggart, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Grant Wilkerson, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
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	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
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	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
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	
Rachel Coyne - Texas Reliability Entity, Inc. - 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	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
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	

Marty Hostler - Northern California Power Agency - 5, Group Name NCPA	
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	
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	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
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	

Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
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	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
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	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Becky Webb - Exelon - 6

Answer	
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	
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	
Document Name	

Comment

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

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.Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

5. The SDT is proposing an 18-month implementation plan. Do you agree to the proposed timeframe?

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy would like a 24-month implementation plan to allow for contract revisions for vendors who are storing and analyzing data.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

These modifications create no significant new compliance requirements, but instead add flexibility and clarity for the Responsible Entities. A shorter time window, such as six months, would be more appropriate.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

TVA does not believe 18 months is sufficient time to conduct required evaluation and implementation of required controls and associated processes. Suggest extend to 36 months.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation recommends a 24-month implementation plan to allow entities flexibility to determine the appropriate implementation actions.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Since the proposed changes to CIP-004 and CIP-011 revolve around the use of vendor services, the time to implement will be influenced by whether or not an organization uses or is planning to use vendor services to store, utilize, or analyze BCSI and if so, whether they have proactively implemented any of these controls. In either case, BPA believes 24 months is the minimum necessary due to the need for implementing or modifying contract language.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
The material changes requiring incremental work are in relation to vendor services per CIP-011-2 R1.3. The requirements need clarity as to whether the controls are intended for net new engagements with vendor service providers as of the effective date of the standard or if it applies to pre-existing vendor service providers. There are several other clarity issues that need to be addressed in the standard requirements as per comments BC Hydro provided to the other questions posed by the SDT in this survey.	
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 response to this question is based on our objections to the proposed revisions to CIP-004 and CIP-011.
Likes 0
Dislikes 0
Response
Andrea Barclay - Georgia System Operations Corporation - 4
Answer No
Document Name
Comment
Giving due consideration to the likelihood that Responsible Entities will need to revise their existing BCSI programs to manage such information based on each individual piece of BCSI, instead of based on storage locations or repositories, GSOC would respectfully suggest an implementation period of 24 months.
Likes 0
Dislikes 0
Response
David Jendras - Ameren - Ameren Services - 3
Answer No
Document Name
Comment
We recommend extending the implementation period to 24 months.
Likes 0
Dislikes 0
Response

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management	
Answer	No
Document Name	
Comment	
Since the intent of these changes is to allow for the use of cloud services, the IRC SRC recommends the SDT consider a phased implementation with mandatory compliance at the end of 18 months – following the concepts from the CIP-002-6 implementation plan. This would allow for a quicker adoption where and when possible for entities that choose to adopt cloud services in this capacity.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
Please provide additional guidance on what is required for existing vendors with provisioned BCSI access. This will be helpful in determining implementation requirements.	
Likes 0	
Dislikes 0	
Response	

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO is in support of the below IRC SRC comments: Since the intent of these changes is to allow for the use of cloud services, the IRC SRC recommends the SDT consider a phased implementation with mandatory compliance at the end of 18 months – following the concepts from the CIP-002-6 implementation plan. This would allow for a quicker adoption where and when possible for entities that choose to adopt cloud services in this capacity.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with the MRO NSRF's comments supporting an 18-month implementation period as a “not to exceed.” That said, we request the Standard Drafting Team (SDT) allow for implementation flexibility, i.e. so entities who are able and would like to move to the new version more quickly than 18 months can do so.	
Likes 0	
Dislikes 0	
Response	
Kayleigh Wilkerson - Lincoln Electric System - 5, Group Name Lincoln Electric System	
Answer	No
Document Name	
Comment	
LES supports an 18-month implementation period as a “not to exceed.” That said, we request the Standard Drafting Team (SDT) allow for implementation flexibility, i.e. so entities who are able and would like to move to the new version more quickly than 18 months can do so.	
Likes 0	

Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
For quicker adoption when possible, per Entity phased adoption is desirable. Recommend a phased implementation with mandatory compliance at the end of 18 months – following concepts from the CIP-002-6 implementation plan Request clarification on what is the correct forum (other than the SDT) for discussing implementation plans?	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
PAC agrees with the proposed timeframe.	
Likes 0	

Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment
PG&E believes the 18 month implementation plan is appropriate for the modifications.

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 an 18-month implementation timeline. MPC also requests ERO guidance regarding early implementation of CIP-004-7 and CIP-011-3. An entity should be permitted to implement procedures to meet compliance with the revised requirements and not be held to previous requirements that are due to be retired upon the enforceable date of project 2019-02 when implementing such changes prior to the enforceable date.

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3

Answer	Yes
Document Name	

Comment
Recognizing that each entity is situated differently,the proposed 18 months is enough for AEP, since this will not result in any major changes to processes.

Likes 0	

Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
We support NPCC comments: For quicker adoption when possible, per Entity phased adoption is desirable. Recommend a phased implementation with mandatory compliance at the end of 18 months – following concepts from the CIP-002-6 implementation plan Request clarification on what is the correct forum (other than the SDT) for discussing implementation plans?	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
SDG&E supports EEI's comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes

Document Name	
Comment	
NVE supports an 18-month implementation period.	
Likes 0	
Dislikes 0	
Response	
Larry Snow - Cogentrix Energy Power Management, LLC - 4 - NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
This is a critical during purchase of an entity with little time to implement the needed requirements.	
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	
For quicker adoption when possible, per Entity phased adoption is desirable. Recommend a phased implementation with mandatory compliance at the end of 18 months – following concepts from the CIP-002-6 implementation plan Request clarification on what is the correct forum (other than the SDT) for discussing implementation plans?	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
EEI supports the 18-month implementation plan proposed by the SDT.	
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 Company agrees the 18-month implementation plan is sufficient.	
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 Comment Form submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
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	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
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	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
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	
Tim Womack - Puget Sound Energy, Inc. - 3	
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	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
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	
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	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Marty Hostler - Northern California Power Agency - 5, Group Name NCPA	
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	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
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	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
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	
Jack Cashin - American Public Power Association - 4	
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	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
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	
Carl Pineault - Hydro-Qu?bec Production - 5	
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	

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Bryan Taggart, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Grant Wilkerson, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL	
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	
Kinte Whitehead - Exelon - 3	
Answer	
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	
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	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

6. The SDT proposes that the modifications in CIP-004 and CIP-011 meet the project scope in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

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

Answer	No
Document Name	

Comment

Clarity is needed to meet the project scope in a cost-effective manner. If encryption for BCSI stored in the cloud is an effective requirement even if the written requirement is more general, that is difficult for entities to follow and know they are compliant. It introduces compliance risk if entities make decisions based on an unclear requirement, and entities may think they are saving money by implementing a non-technical solution but that could backfire if a technical solution is actually required to be sufficient.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

ITC supports the Comment Form submitted by EEI

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

Due to the endless possibilities of 3rd party storage solutions/vendor services for storage, we do not feel CIP-011 R1.3 is necessary and is exceedingly burdensome. If the currently written controls in R1.4 are implemented, the electronic technical mechanisms are sufficient to protect BCSI from unauthorized access.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

CAISO is in support of the IRC SRC comments:

The costs to implement the changes cannot be calculated as the standards are currently written; however, there are several areas where proposed modifications unnecessarily increase cost. We would require a better understanding of the term “provisioning” and the context of how the concepts outlined in both standards would apply in a use case where third party providers of services are going to be used to store or process BCSI information.

In the spirit of cost-effectiveness, the IRC SRC respectfully requests the SDT consider the following opportunities to consolidate requirements and/or eliminate duplication and overlap under CIP-004.

Introduction of “provisioning” not commensurate with cost – the proposed change from BCSI designated storage locations to personnel with provisioned access to BCSI creates significant administrative overhead for entities and is not commensurate with the security value achieved. The technical rationale identifying repositories for BCSI in the current standards vs “provisioned access” appears to be the same when you review information in the technical rationale narrative.

Opportunity to consolidate CIP-004 requirements - The addition of proposed new requirement, R6, would require entities to implement an access management program for ***BES Cyber System Information (BCSI; i.e. information)*** on par with the existing (and proposed continuation of) requirement, R4, to implement an access management program for ***BES Cyber Systems (BCS; i.e. assets)***, i.e., to identify, authorize and track provisioned and authorized personnel with access to BCSI - both hard-copy and electronic copy – at the entity’s managed location and at 3rd party storage locations (aka “cloud”) as well.

For entities using or considering a move to 3rd party cloud storage without encryption of BCSI (such as MS Office 365), entities will be required to obtain a list of 3rd party cloud personnel such as systems administrators with Administrative level privileges to systems which store an entity’s BCSI – which may also be replicated at multiple cloud data centers and multiple sets of personnel. This is not sustainable. To address this, and in keeping with the criteria of NERC’s Standards Efficiency Review, the IRC SRC proposes requirement R6 be consolidated into R4, so entities are only required to implement to a single access management program.

Finally, the wording of CIP-004-7, Part 6.2 expands the scope of the 15-month review (i.e. to verify the *need* for continued access) to include the quarterly review performed under Part 4.2 (i.e. to verify that provisioned access is *authorized*). To eliminate duplication, Part 6.2 should be reworded to mirror that of CIP-004-6, Part 4.4 (i.e. to verify that access is correct and necessary for performing assigned work functions).

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	
Comment	
We support NPCC Regional Standards Committee comments	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
Business agreements with vendors requiring vulnerability and breach disclosures, as well as incident response, may not be cost-effective (or possible) to establish.	
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	No
Document Name	
Comment	
Based on our response to question 1, we believe that a more cost effective approach exists to enable use of third party services for storage and analysis of BCSI in a secure manner without introducing additional compliance burden on entities. The proposed revisions should not introduce additional requirements or compliance burden for those entities that do not plan to utilize third party services for storage or analysis of BCSI. In addition, we encourage a risk-based approach to address prevention of unauthorized access to BCSI while stored in third party environment or being processed by third-party. See our response to Question 3. A "cost-effective" approach would be for NERC to agree to rely on independent audit reports (eg SOC2 Type2)	

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The costs to implement the changes cannot be calculated as the standards are currently written; however, there are several areas where proposed modifications unnecessarily increase cost. We would require a better understanding of the term “provisioning” and the context of how the concepts outlined in both standards would apply in a use case where third party providers of services are going to be used to store or process BCSI information.

In the spirit of cost-effectiveness, the IRC SRC respectfully requests the SDT consider the following opportunities to consolidate requirements and/or eliminate duplication and overlap under CIP-004.

Introduction of “provisioning” not commensurate with cost – the proposed change from BCSI designated storage locations to personnel with provisioned access to BCSI creates significant administrative overhead for entities and is not commensurate with the security value achieved. The technical rationale identifying repositories for BCSI in the current standards vs “provisioned access” appears to be the same when you review information in the technical rationale narrative.

Opportunity to consolidate CIP-004 requirements - The addition of proposed new requirement, R6, would require entities to implement an access management program for ***BES Cyber System Information (BCSI; i.e. information)*** on par with the existing (and proposed continuation of) requirement, R4, to implement an access management program for ***BES Cyber Systems (BCS; i.e. assets)***, i.e., to identify, authorize and track provisioned and authorized personnel with access to BCSI - both hard-copy and electronic copy – at the entity’s managed location and at 3rd party storage locations (aka “cloud”) as well.

For entities using or considering a move to 3rd party cloud storage without encryption of BCSI (such as MS Office 365), entities will be required to obtain a list of 3rd party cloud personnel such as systems administrators with Administrative level privileges to systems which store an entity’s BCSI – which may also be replicated at multiple cloud data centers and multiple sets of personnel. This is not sustainable. To address this, and in keeping with the criteria of NERC’s Standards Efficiency Review, the IRC SRC proposes requirement R6 be consolidated into R4, so entities are only required to implement to a single access management program.

Finally, the wording of CIP-004-7, Part 6.2 expands the scope of the 15-month review (i.e. to verify the *need* for continued access) to include the quarterly review performed under Part 4.2 (i.e. to verify that provisioned access is *authorized*). To eliminate duplication, Part 6.2 should be reworded to mirror that of CIP-004-6, Part 4.4 (i.e. to verify that access is correct and necessary for performing assigned work functions).

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment
NV Energy does not agree. The modifications as proposed by the SDT do not meet the project scope in a cost-effective manner. These modifications depend on established and/or modified vendor relationships that are being addressed outside of scope. This goes beyond the scope identified by the FERC Order for CIP-004 & CIP-011 in Project 2019-02. Granting access to individual pieces of information is not cost effective, would be resource intensive, and is not in line with industry best practices. The new language in CIP-011 could result in required audits of third parties. CIP-013 doesn't require audits of vendor performance and adherence, where CIP-011 without similar exception would require these types of verifications for compliance. This is beyond the scope of the NERC CIP Standards to audit external third parties compliance to the requirements, thus requiring undue burden on the Responsible Entity.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	

Comment
The SDT needs to provide a cost/benefit analysis in order for us to determine if their proposal is cost effective. Also see SMUDs comments.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	

Comment
Support the MRO-NSRF comments.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	
Comment	

As discussed above, the proposed revisions increase the scope of applicability, ambiguity, compliance activities, and burden without the likelihood of an associated increase in reliability or security and with the potential to create a security gap related to the management and protection of BCSI. Moreover, the driver for these revisions do not impact all Responsible Entities. Accordingly, without appropriate backwards compatibility, Responsible Entities with existing, effective programs and no cloud or other third-party hosted services will be required to expend significant resources to ensure compliance.

This creates uncertainty and increases the burden of compliance on Responsible Entities for no ostensible enhancement to reliability or security. Taken together, the proposed revisions do not propose substantive enhancements to security or reliability that would justify the additional cost, resource, or compliance burden or risk for a large number of Responsible Entities.

Likes 0	
Dislikes 0	
Response	

Jack Cashin - American Public Power Association - 4

Answer	No
Document Name	
Comment	

The current modifications to CIP-004 and CIP-011 do not meet the project scope in a cost-effective way. This is because there are elements of the changes to CIP-011 (see answer to question 7 below) that are supply chain risks that should be addressed in CIP-013 (Project 2019-03) rather than in Project 2019-02. Adding the level of Supply Chain Risk Management proposed within CIP-011 R1 Part 1.3, unecessarily adds significant implementation and cost burden. Inefficiencies will result from unecessary commingling of requirements for Projects 2016-02, 2019-02 and 2019-03.

Likes 0	
Dislikes 0	
Response	

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

Answer	No
Document Name	
Comment	

Due to the endless possibilities of 3rd party storage solutions/vendor services for storage, we do not feel CIP-011 R1.3 is necessary and is exceedingly burdensome. If the currently written controls in R1.4 are implemented, the electronic technical mechanisms are sufficient to protect BCSI from unauthorized access.

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

It is N&ST's understanding that the primary goal of this project is to clarify requirements to prevent unauthorized access to BCSI while "in storage" in order to facilitate the use of 3rd-party storage solutions, including cloud-based services. If that understanding is correct, N&ST believes total rewrites of long-standing Information Protection Program and BCSI storage location access management requirements are neither necessary nor desirable.

N&ST believes adding a single, simply-worded requirement to either CIP-004 or CIP-011, stating that all "designated storage locations" must have documented technical controls that prevent unauthorized access to BCSI, would be quite sufficient.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Regarding CIP-011-3 R1 Part 1.3, the terminology for the sub-parts do not add value to CIP-011. It is unclear what this terminology would require or what any of these terms mean, making them subject to broad and differing interpretation. This proposed requirement is a paperwork exercise that adds administrative burden without realizing security benefits. Auditability will be difficult and open to interpretation. For these reasons, MPC does not consider these changes to be cost-effective.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Technology and costs are ever evolving in this area and without NERC performing a cost benefit analysis it is impossibkle to judge the impact ofthis specific proposal.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
PG&E at this time cannot determine if the modifications are cost effective. PG&E would like to have an option to select Unknown, instead of just Yes and No.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5, Group Name NCPA	
Answer	No
Document Name	
Comment	
The SDT needs to provide a cost/benefit analysis in order for us to determine if their proposal is cost effective. Also see SMUDs comments.	
Likes 0	
Dislikes 0	

Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

As mentioned in question 1, changing the term from “designated storage locations” to “provisioned access” adds administrative work to update program documents and access tracking tools, without a commensurate increase in flexibility or security. CIP-011 R1.3 and R1.4 expand the scope of the SAR to include more than just cloud service providers and for medium impact without ERC. This is a significant expansion of scope that is not cost effective.

The existing versions of the CIP standards already take into consideration potential cloud service providers. One approach could be to allow current versions to remain effective, while offering the new versions to entities that want to implement them, as is being done with PRC-005 versions -1.1b and -6.

Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	

As mentioned in question 1, changing the term from “designated storage locations” to “provisioned access” adds administrative work to update program documents and access tracking tools, without a commensurate increase in flexibility or security. CIP-011 R1.3 and R1.4 expand the scope of the SAR to include more than just cloud service providers and for medium impact without ERC. This is a significant expansion of scope that is not cost effective.

The existing versions of the CIP standards already take into consideration potential cloud service providers. One approach could be to allow current versions to remain effective, while offering the new versions to entities that want to implement them, as is being done with PRC-005 versions -1.1b and -6.

Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No

Document Name	
Comment	
BC Hydro has insufficient information to determine how cost effective these modifications are. For additional details, please reference BC Hydro's comments to the other questions in this survey.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
This is very difficult to quantify across all of industry and various types of registered entities. If the language can be adjusted to account for non-electronic information storage locations, it has potential.	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
Answer	No
Document Name	
Comment	
Based on our response to question 1, we believe that a more cost effective approach exists to enable use of third party services for storage and analysis of BCSI in a secure manner without introducing additional compliance burden on entities. The proposed revisions should not introduce additional requirements or compliance burden for those entities that do not plan to utilize third party services for storage or analysis of BCSI. In addition, we encourage a risk-based approach to address prevention of unauthorized access to BCSI while stored in third party environment or being processed by third-party. See our response to Question 3.	
Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

PAC does not agree. The modifications as proposed by the SDT do not meet the project scope in a cost-effective manner. These modifications depend on established and/or modified vendor relationships that are being addressed outside of scope. This goes beyond the scope identified by the FERC Order for CIP-004 & CIP-011 in Project 2019-02. Granting access to individual pieces of information is not cost effective, would be resource intensive, and is not in line with industry best practices.

The new language in CIP-011 could result in required audits of third parties. CIP-013 doesn't require audits of vendor performance and adherence, where CIP-011 without similar exception would require these types of verifications for compliance. This is beyond the scope of the NERC CIP Standards to audit external third parties compliance to the requirements, thus requiring undue burden on the Responsible Entity.

Likes 0	
Dislikes 0	
Response	

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

As our comments in question 1, changing the term from "designated storage locations" to "provisioned access" adds administrative workload to update program documents and manage additional access to BCSI that is not manageable without an automated tool. We suggest using BCSI Repository approach to manage BCSI access as our comments in question 1. By using this approach, there is no additional cost for the ongoing compliance and the CIP-006 Part R16. 4.1 we suggest will address the cloud storage third-party access to BCSI.

Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	

To minimize churn among standard versions, Reclamation recommends the SDT take additional time to coordinate the modifications in CIP-004-7 and CIP-011-3 with other existing drafting teams for related standards. This will help minimize the costs associated with the planning and adjustments required to achieve compliance with frequently changing requirements. NERC should foster a standards development environment that will allow entities to fully implement technical compliance with current standards before moving to subsequent versions. This will provide entities economic relief by better aligning the standards for overall improved reliability and by reducing the chances that standards will conflict with one another.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Under the existing version of the standards entities are already required to apply protection mechanisms to BSCI when shared. If requirement R1.3 remains it should not be applied retroactively to vendors.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No
Document Name	

Comment

The current approach would be resource intensive and difficult to manage. Many of the new requirements are also vague and broad. This could make it very difficult to come up with solutions to meet the requirement and may cost much more to implement than it would if the requirements and measures were clearer. Given the ambiguity, it is hard to imagine how the regional entities will interpret the requirements and how that would impact the implementation.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy does not agree. It is not clear the extent of changes that may be necessary to existing methods that are already effectively protecting BCSI and to what extent those changes will result in additional risk reduction.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
As written, R1.4 and R1.5 will apply to all vendors that also may utilize or analyze BCSI. This would mean that entities would have to utilize resources to identify/assess risks (R1.4) and would be required to develop/purchase/implement tools to ensure that at least one or more documented electronic technical mechanisms to protect BCSI (R1.5). While this makes sense when utilizing third-party solutions such as cloud services, these extra requirements for vendors that simply need to access physical or electronic documentation containing BCSI or that utilize this type of information onsite on a periodic basis appears unnecessary and costly to implement.	
Likes 0	
Dislikes 0	
Response	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
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 has no comments on the project scope cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3	
Answer	Yes
Document Name	
Comment	
Again, recognizing that each entity is situated differently,the proposed revisions can likely be implemented by AEP in a cost effective manner, since this will not result in any major changes to processes.	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
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	

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Snow - Cogentrix Energy Power Management, LLC - 4 - NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
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	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 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	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Bryan Taggart, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Grant Wilkerson, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL	
Answer	
Document Name	
Comment	
No position.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
None	

Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	
Document Name	
Comment	
SDG&E has no comment on the cost effectiveness of the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	
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	
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	
Document Name	
Comment
Exelon has elected to align with EEI in response to this question.
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
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

David Rivera - New York Power Authority - 3	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	

7. Provide any additional comments for the standard drafting team to consider, if desired.	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
Technical rationale for CIP-011, part 1.4, implies there would always be the state "use" in all vendor solutions. However, in Tri-State's experience that is not always the case, and also depends on the individual's interpretation of what "use" of BCSI means. A common example where there would not be "use" in the cloud is backup storage. (Where the data is sent already encrypted and in order to use it (aka restore) has to be called back to the customer's premises to be unencrypted.) Recommend the SDT remove "use", or instead change the entire paragraph to refer to the lifecycle of the data from transit to disposal.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	
Document Name	
Comment	
none at this time, thank you.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	
Document Name	
Comment	
The language is not clear on whether existing vendors will be subject to the new R1.4 and R1.5 requirements or if this will apply only to new vendors after the future enforcement date.	

The R1.4 language "identify and assess" is similar to CIP-013, which entities are finding requires a significant amount of resources to approrpriately comply with.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino	
Answer	
Document Name	
Comment	
Granting access to individual pieces of information is not cost effective, would be resource intensive, and is not in line with industry best practices. The approach of managing access to repositories was a more practical approach and was more manageable as well.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	
Document Name	
Comment	

I support the draft CIP-004-7 Standard, however there sonsistent use of defined terms could be implemented. BES Cyber System Information is established as the anacronym (BCSI) in R2.1, yet it is not used in R6, M6, or Table R6 title.

Conducting CIP-013 vendor risk assessments is a new process for many entities, it would just add additional confusion to have risk assessment requirements in standards other than CIP-013. The risk assessment required by draft Standard CIP-011-3 R1.3 should be omitted and moved to CIP-013.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	
Document Name	

Comment

The NIST framework adequately addresses these Standards as they pertain to all BES Cyber Systems. The NIST framework is sufficient for guiding federal entities' security efforts pertaining to the Bulk-Power System, rather than creating duplicative requirements in the CIP standards. NERC should leverage and incorporate the existing NIST framework, instead of creating additional, identical requirements in the form of CIP standards. Additional, identical requirements create an administrative burden without improving overall security posture, thereby creating the potential for security failures because of the required inefficient use of resources.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	
Document Name	

Comment

We suggest removing CIP-011 Part 1.3 and P1.4 as our comments in question 3. Define a BCSI Repository term in CIP-011 and use it for the BCSI access management in CIP-004. Given that BCSI must have a home, there is no access control basis unless a BCSI repository is identified.

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	
Document Name	
Comment	
Puget Sound Energy supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	

David Rivera - New York Power Authority - 3	
Answer	
Document Name	
Comment	
General comment - Request consistent language in the (CIP-011) Measures. Parts 1.1, 1.2, 2.1, and 2.2 start with “Examples of acceptable evidence include, but are not limited to, the following:.” Parts 1.3 and 1.4 start with “Examples of acceptable evidence may include, but are not limited to, dated documentation of the following:.” Part 1.3 is consistent with other Standards. Next, some Parts explicitly end each bullet with “or.” Some Parts are silent on how to read their bullets (or vs and). Request explicit consistency. Request consistent redlines because the CIP-011 redline-to-last-approved is not consistent with the CIP-011 redline-to-last-posted	
Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	
Comment	
Please copy applicabilty and change where appropriate for each part, such as done in CIP-011 R1	

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	
Document Name	

Comment

1. CIP-011 R1.3 is more appropriate to be located in CIP-013.
2. CIP-004-7 addresses access management controls for BCSI in relation to Medium Impact with ERC BES Cyber Systems and associated EACMS and PACS; however, CIP-011-3 is broader in scope to include Medium Impact BES Cyber Systems and associated EACMS and PACS without limiting coverage to ERC only. Why is there a discrepancy?

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

The standards drafting team has not provided enough justification for the new CIP-011-3 R1.3 and 1.4 vendor management requirements. The existing CIP requirements already require protection of BCSI, including BCSI stored, analyzed and used by vendors. The drafts would require almost the same level of protections as those required for BES Cyber Assets in CIP-013-1.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

The standards drafting team has not provided enough justification for the new CIP-011-3 R1.3 and 1.4 vendor management requirements. The existing CIP requirements already require protection of BCSI, including BCSI stored, analyzed and used by vendors. The drafts would require almost the same level of protections as those required for BES Cyber Assets in CIP-013-1.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

CEHE noticed that CIP-004-7 Requirement R6 does not consider revocation when an individual is reassigned or transferred, in a similar way in which it is accounted for in Requirement R5 Part 5.2.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5, Group Name NCPA

Answer	
Document Name	

Comment

No.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

PG&E has no additional input.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

Minnkota respectfully states that it is opposed to changing the CIP Standards Requirements table column from “Applicable Systems” to “Applicability”. This could also be confused with the Applicability in section A.4. of the standard. While we appreciate the SDT’s attempt to clarify that the requirement is applicable to BCSI about those systems, regardless of if it is stored in those same systems or elsewhere, we propose that this be done in the requirement language instead. We submit for the SDT’s consideration the following proposal:

CIP-004
6.1 Remove “BCSI associated with:” in Applicability column. Change column heading back to Applicable Systems. Change requirement to “Authorize based on need, as determined by
the Responsible Entity, provisioneding of access to BCSI pertaining to applicable systems,
except for CIP Exceptional Circumstances.”
6.2 Remove “BCSI associated with:” in Applicability column. Change column heading back to Applicable Systems. Change requirement to “Verify at least once every 15 calendar months that all provisioned access to BCSI pertaining to applicable systems:”
6.3 Remove “BCSI associated with:” in Applicability column. Change column heading back to Applicable Systems. Change requirement to “For termination actions, remove the individual’s ability to use provisioned access to BCSI pertaining to applicable systems . . .”

CIP-011
1.1 Remove “BCSI pertaining to:” in Applicability column. Change column heading back to Applicable Systems. Change Requirement to “Method(s) to identify BCSI pertaining to applicable systems.”
1.2 Revert Applicability column back to currently enforceable. Change Requirement to “Method(s) to protect and securely handle BCSI pertaining to applicable systems.”

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3

Answer	
Document Name	

Comment

No further comment.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	
Document Name	

Comment

No aditional comments

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

We thank you for this opportunity to 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	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE continues to be concerned about the applicability in CIP-004-7 R4 and R5, and the use of encryption as stated in CIP-011-3. Additionally, Texas RE is concerned with the removal of key management in CIP-011-3. Regarding applicability, Texas RE recommends the standard drafting team (SDT) update the Applicable Systems columns in CIP-004-7 R4 (Parts 4.1-4.3) and R5 (Parts 5.1-5.4), to

Medium Impact BES Cyber Systems and their associated:

1. EACMS;
2. PACS; and
3. PCAs.

Since CIP-011-3 Parts 2.1 and 2.2 includes EACMS, PACS, and PCA, this change would align CIP-004-7 better with CIP-011-3 as well as improve an overall security posture for access management and revocation.

Regarding encryption, Texas RE continues to be concerned that entities could simply use the bare minimum encryption controls in accordance with CIP-011-3 R1.4. Neither CIP-004 nor CIP-011 contain requirement language specifying a minimum acceptable level of encryption where encryption is used. The absence of enforceable language results in any encryption algorithm at any key strength, including those algorithm and key strength combinations that have been determined to not be sufficiently strong, meeting compliance with this requirement as it is written. This may result in inconsistent enforcement of this requirement across the regions.

Texas RE suggests writing additional Part to CIP-011-3 Requirement R1:

Part 1.5 – For those methods identified in Part 1.4 that use encryption, utilize an encryption key strength of at least 128 bits.

This language is consistent with the NIST framework for medium-impact information and does not mandate the use of encryption. If encryption is used, however, it provides clear criteria as to what level of encryption is considered acceptable. The inclusion of minimal key strength criteria also squares with FERC's observations in its 2018 Staff Report, Lessons Learned from Commission-Led CIP Reliability Audits that select entities could improve their security posture by enhancing their encryption key strength.

Regarding key management, Texas RE is concerned with the removal of key management process(es) in CIP-011-3, Requirement R2, part 2.1. Key management is an important part of encryption and reduces the risk of unauthorized electronic access. Key management is also an important control when implementing third-party cloud service providers. If personnel have access to the encryption keys, they have electronic access to BCSI.

Texas RE has the following additional comments:

- Texas RE inquires as to the difference between the terms “provisioning of access” and “provisioned access”, which are used in CIP-004-7 R6 and the term “access”, which is used in R4 and R5.
- In the measure for CIP-011-3 R1 Part 1.3, Texas RE recommends changing “or” to “and”. Vendor certification alone is insufficient to verify vendor controls. Entities should have vendor certification and Registered Entity verification of vendor controls.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	
Document Name	

Comment

ATC thanks the SDT for mindfully approaching the directives of this FERC Order so as to enable the CIP Standards for emerging technologies like off-premises BCSI cloud solutions/platforms, while maintaining backwards compatibility for on-premises BCSI solutions. Permitting the CIP Standards to stall and lag behind emerging/advancing technology disincentivizes the growth and maturity of our most critical infrastructure; which in and of itself breeds a security and reliability risk. Thank you also for the continued investment in the supporting materials like IG and TR; this truly helps provide a common understanding.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	
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	
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	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	

APPA agrees with the CIP-011 R1 Parts 1.1, 1.2 and 1.4 revisions. Requirement 1 Part 1.3 is a supply chain risk management requirement and CIP-011 should address only information security. The R1, Part 1.3 is a supply chain risk management provision that is more aptly dealt with in CIP-013. The language included in CIP-011 is not intended to require technical controls supporting the management of supply chain risk.

Public power finds the that current language of CIP-013 would provide the necessary clarity to implement the vendor assessment practices suggested in R1, Part 1.3. While the measures do provide some guidance, the measures are not part of the requirement language in R1, Part 1.3. The R1, Part 1.3 proposed language reads like a new requirement rather than something that complements CIP-013 practices.

The RI, Part 1.3 language suggests a gap that needs to be addressed in CIP-013. Attempting to address the risk inappropriately in CIP-011 would only set up future corrections.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	
Document Name	

Comment

Support the MRO-NSRF comments.

Likes 0	
Dislikes 0	

Response

Larry Snow - Cogentrix Energy Power Management, LLC - 4 - NPCC,SERC,RF

Answer	
Document Name	

Comment

Better detail and clarifications are needed throughout multiple sections of the document.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

General comment – The IRC SRC requests consistent language in the (CIP-011) Measures. Parts 1.1, 1.2, 2.1, and 2.2 start with “Examples of acceptable evidence include, but are not limited to, the following:” Parts 1.3 and 1.4 start with “Examples of acceptable evidence may include, but are not limited to, dated documentation of the following:.” Part 1.3 is consistent with other Standards. Next, some Parts explicitly end each bullet with “or.” Some Parts are silent on how to read their bullets (or vs and). Request explicit consistency.

CIP-011 Part 1.3’s requirement includes “implement risk management method(s).” However the corresponding measures says “Implementation of the risk identification and assessment method(s) (1.3).” Consistency between the requirement and measure would reduce the risk of confusion. We would prefer the use of the terms “risk identification and assessment” as opposed to “risk management.” Risk management is generally understood to include many things. Request consistent redlines because the redline-to-last-approved is not the same redline-to-last-posted for CIP-011.

The standards drafting team has not provided enough justification for the new CIP-011-3 R1.3 and 1.4 vendor management requirements. The existing CIP requirements already require protection of BCSI, including BCSI stored, analyzed and used by vendors. The drafts would require almost the same level of protections as those required for BES Cyber Assets in CIP-013-1. To address this, the IRC SRC requests the SDT consider incorporating any necessary provisions into CIP-013.

Finally, the wording of CIP-004-7, Part 6.2 expands the scope of the 15-month review (i.e. to verify the *need* for continued access) to include the quarterly review performed under Part 4.2 (i.e. to verify that provisioned access is *authorized*). To eliminate duplication, Part 6.2 should be reworded to mirror that of CIP-004-6, Part 4.4 (i.e. to verify that access is correct and necessary for performing assigned work functions).

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

General comment - Request consistent language in the (CIP-011) Measures. Parts 1.1, 1.2, 2.1, and 2.2 start with “Examples of acceptable evidence include, but are not limited to, the following:.” Parts 1.3 and 1.4 start with “Examples of acceptable evidence may include, but are not limited to, dated documentation of the following:.” Part 1.3 is consistent with other Standards. Next, some Parts explicitly end each bullet with “or.” Some Parts are silent on how to read their bullets (or vs and). Request explicit consistency.

Request consistent redlines because the CIP-011 redline-to-last-approved is not consistent with the CIP-011 redline-to-last-posted

Since technological solutions are often the answer to the various challenges of the electrical industry, there is a tendency to resort to cloud computing solutions to accelerate deployment and reduce costs. It therefore appears important to us, in order to reduce cybersecurity risks to a minimum while ensuring the flexibility required by maintaining the reliability of the Bulk Electric System that NERC focus on adapting the CIP Reliability Standards to cloud computing environments. Exploring ways to integrate certifications (i.e. FedRamp, or Soc II Type 2) will be essential to permit compliance certification with the CIP requirements by various cloud providers. This support would prevent entities from needing to carry out isolated proceedings with suppliers, which may be inconsistent across industry.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

CIP-011 Requirement 1.3 does not cleary identify what the requriment is. The measure is providing the clarity.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	

Monika Montez - California ISO - 2 - WECC

Answer	
Document Name	
Comment	

CAISO is in support of the below IRC SRC comments:

General comment – The IRC SRC requests consistent language in the (CIP-011) Measures. Parts 1.1, 1.2, 2.1, and 2.2 start with “Examples of acceptable evidence include, but are not limited to, the following:” Parts 1.3 and 1.4 start with “Examples of acceptable evidence may include, but are not limited to, dated documentation of the following:.” Part 1.3 is consistent with other Standards. Next, some Parts explicitly end each bullet with “or.” Some Parts are silent on how to read their bullets (or vs and). Request explicit consistency.

CIP-011 Part 1.3’s requirement includes “implement risk management method(s).” However the corresponding measures says “Implementation of the risk identification and assessment method(s) (1.3).” Consistency between the requirement and measure would reduce the risk of confusion.

We would prefer the use of the terms “risk identification and assessment” as opposed to “risk management.” Risk management is generally understood to include many things.

Request consistent redlines because the redline-to-last-approved is not the same redline-to-last-posted for CIP-011.

The standards drafting team has not provided enough justification for the new CIP-011-3 R1.3 and 1.4 vendor management requirements. The existing CIP requirements already require protection of BCSI, including BCSI stored, analyzed and used by vendors. The drafts would require almost the same level of protections as those required for BES Cyber Assets in CIP-013-1. To address this, the IRC SRC requests the SDT consider incorporating any necessary provisions into CIP-013.

Finally, the wording of CIP-004-7, Part 6.2 expands the scope of the 15-month review (i.e. to verify the *need* for continued access) to include the quarterly review performed under Part 4.2 (i.e. to verify that provisioned access is *authorized*). To eliminate duplication, Part 6.2 should be reworded to mirror that of CIP-004-6, Part 4.4 (i.e. to verify that access is correct and necessary for performing assigned work functions).

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 thank you for this opportunity to comment.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	
Southern does not have any additional comments other then those stated in the previous questions.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Bryan Taggart, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Grant Wilkerson, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	