Comment Report

Project Name:	2019-02 BES Cyber System Information Access Management
Comment Period Start Date:	12/20/2019
Comment Period End Date:	2/3/2020
Associated Ballots:	2019-02 BES Cyber System Information Access Management CIP-004-7 IN 1 ST 2019-02 BES Cyber System Information Access Management CIP-011-3 IN 1 ST 2019-02 BES Cyber System Information Access Management Implementation Plan IN 1 OT

There were 91 sets of responses, including comments from approximately 209 different people from approximately 131 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The proposed revision to Requirement R1 Part 1.1 adds the requirement to identify BCSI storage locations. Do you agree that the requirement as written allows the Responsible Entity the flexibility to identify which storage locations are for BCSI? Do you agree the requirement is necessary? If you disagree with the changes made, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

2. The standard drafting team (SDT) attempted to maintain backwards compatibility with concepts of designated storage locations and access-level requirements previously contained in CIP-004-6. Do you agree that there is a minimal effort to meet this objective while providing greater clarity between BCSI and BES Cyber System (BCS) requirement obligations?

3. The SDT is attempting to expand information storage solutions or security technologies for Responsible Entities. Do you agree that this approach is reflected in the proposed requirements?

4. The SDT is addressing, and further defining, the risk regarding potential compromise of BCSI through the inclusion of the terms "obtain" and "use" in requirement CIP-011-3, Requirement R1 Part 1.2. Do you agree that this will more accurately address the risk related to the potential compromise of BCSI versus the previous approach?

5. The SDT is proposing to have BCSI in the "Applicability" column. Do you agree that this provides better clarity on the focus of the requirements?

6. The SDT is proposing to address the security risks associated with BCSI environments, particularly owned or managed by vendors via CIP-011-3, Requirements R1, Part 1.4, and Requirement R2, Parts 2.1 and 2.2. Do you agree that these requirements will promote a better understanding of security risks involved while also providing opportunities for the Responsible Entity to address appropriate security controls?

7. The SDT is addressing the growing demand for Responsible Entities to leverage new and future technologies such as cloud services. Do you agree that the proposed changes support this endeavor?

8. The SDT is proposing a new "key management" set of requirements. Do you agree that key management involving BCSI is integral to protecting BCSI?

9. The SDT is proposing to shift the focus of security of BCSI more towards the BCSI itself rather than physical security or "hardware" storage locations. Do you agree that this approach aids the Responsible Entity by reducing potential unneeded controls on BCS?

10. The SDT is proposing to transfer all BCSI-related requirements from CIP-004 to CIP-011 with the understanding that this will further address differing security needs between BCSI and BCS as well as ease future standard development. Do you agree that this provides greater clarity between BCSI and BCS requirements?

11. The SDT increased the scope of information to be evaluated by including both Protected Cyber Assets and all Medium Impact (not just Medium Impact Assets with External Routable Connectivity). Are there any concerns regarding a Responsible Entity attempting to meet these proposed, expanded requirements?

12. In looking at all proposed recommendations from the SDT, are the proposed changes a cost-effective approach?

13. Do you have any other general recommendations/considerations for the drafting team?

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
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
Santee Cooper	Chris Wagner	1		Santee Cooper	Rene' Free	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC
MRO	Dana Klem	1,2,3,4,5,6	MRO	MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administration	1,6	MRO
					Andy Crooks	SaskPower Corporation	1	MRO
					Bryan Sherrow	Kansas City Board of Public Utilities	1	MRO
					Bobbi Welch	Omaha Public Power District	1,3,5,6	MRO

					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					Bobbi Welch	Midcontinent ISO	2	MRO
					Douglas Webb	Kansas City Power & Light	1,3,5,6	MRO
					Fred Meyer	Algonquin Power Co.	1	MRO
					John Chang	Manitoba Hydro	1,3,6	MRO
					James Williams	Southwest Power Pool, Inc.	2	MRO
					Jamie Monette	Minnesota Power / ALLETE	1	MRO
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO
					Sing Tay	Oklahoma Gas & Electric	1,3,5,6	MRO
					Terry Harbour	MidAmerican Energy	1,3	MRO
					Troy Brumfield	American Transmission Company	1	MRO
PPL - Louisville Gas and Electric Co.	Devin Shines	1,3,5,6	RF,SERC	PPL NERC Registered Affiliates	Brenda Truhe	PPL Electric Utilities Corporation	1	RF
					Charles Freibert	PPL - Louisville Gas and Electric Co.	3	SERC
					JULIE HOSTRANDER	PPL - Louisville Gas and Electric Co.	5	SERC
					Linn Oelker	PPL - Louisville Gas and Electric Co.	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
	Holly Chaney	3		SNPD Voting Members	John Martinsen	Public Utility District No. 1	4	WECC

Snohomish County PUD No. 1						of Snohomish County		
					John Liang	Snohomish County PUD No. 1	6	WECC
					Sam Nietfeld	Public Utility District No. 1 of Snohomish County	5	WECC
					Long Duong	Public Utility District No. 1 of Snohomish County	1	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Amber Skillern	East Kentucky Power Cooperative	1	SERC
					Jennifer Brey	Arizona Electric Power Cooperative	1	WECC
					Joseph Smith	Prairie Power , Inc.	1,3	SERC
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		DTE Energy - DTE Electric	Jeffrey Depriest	DTE Energy - DTE Electric	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF

					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
					Mark Garza	FirstEnergy- FirstEnergy	4	RF
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,RF,SERC	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		Public Utility District No. 1 of Chelan County	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Ginette Lacasse	Public Utility District No. 1 of Chelan County	1	WECC
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	PG&E	PG&E	1	WECC
					PG&E	PG&E	3	WECC
					PG&E	PG&E	5	WECC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
Eversource Energy	Quintin Lee	1		Eversource Group	Sharon Flannery	Eversource Energy	3	NPCC

					Quintin Lee	Eversource Energy	1	NPCC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no NextEra	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	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
					Sean Cavote	PSEG	4	NPCC
					Kathleen Goodman	ISO-NE	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
					Mike Forte	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
					Ashmeet Kaur	Con Ed - Consolidated Edison	5	NPCC
					Caroline Dupuis	Hydro Quebec	1	NPCC
					Chantal Mazza	Hydro Quebec	2	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					Laura McLeod	NB Power Corporation	5	NPCC
					Randy MacDonald	NB Power Corporation	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					John Hastings	National Grid	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
Portland General Electric Co.	Ryan Olson	5		PGE Group 2	Angela Gaines	Portland General Electric Co.	1	WECC
					Dan Zollner	Portland General Electric Co.	3	WECC

					Daniel Mason	Portland General Electric Co.	6	WECC
					Ryan Olson	Portland General Electric Co.	5	WECC
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
Lower Colorado River Authority	Teresa Cantwell	1,5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE
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. The proposed revision to Requirement R1 Part 1.1 adds the requirement to identify BCSI storage locations. Do you agree that the requirement as written allows the Responsible Entity the flexibility to identify which storage locations are for BCSI? Do you agree the requirement is necessary? If you disagree with the changes made, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	No
Document Name	

Comment

I don't see the referenced changes in CIP-004-7. If you are refering to CIP-011-3, "storage locations" is very broad. This could be a problem during audits, if the auditor does not like the interpretation. We need a much stricter wording for storage locations.

Likes 1	Miller Scott On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1;
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

It is already implied in CIP-004 R4 that storage locations have to be identified and adds to the complexity of the compliance requirement. Flexibility is already provided under CIP-004 R4. Access controls were grouped in CIP-004 R4, relocating these controls to CIP-011 creates additional complexities.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

An overarching problem with this proposed draft of CIP-011-3 is the removal of the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems in CIP-011-3 R1.1 as currently provided in CIP-004-6 R4.1, and how this greatly and needlessly expands the scope of all subsequent parts of R1, and R2.

Identifying BCSI storage locations for system information pertaining to Medium Impact BES Cyber Systems without ERC is not necessary, as Cyber Systems without remote connectivity can only be compromised locally by a breach of physical security. The information protection mandated by this standard will afford no protection should an adversary gain physical access to the Cyber Systems.

We will not be able to vote affirmative unless “with ERC” is added to the Applicability of of Medium Impact BES Cyber Systems in R1 Part 1.1.

We agree that the language provides flexibility in identifying BCSI storage locations.

We would prefer to retain the less prescriptive “Method(s)” over the proposed requirement change to “Process(es).” Making this change to “process” implies that existing programs will need to be updated to a procedural format. Again, this is not requested by the SAR and does not increase reliability, yet this would add administrative burden and increase compliance risk.

To clarify location with respect to electronic storage locations, recommend the definition of “BCSI Repository” per EEI comments along these lines:

“BCSI Repositories are either physical or electronic storage locations where BCSI is retained for long term storage. For physical BCSI Repositories, this would be a physical location. For electronic BCSI Repositories, this would be a logical location. Short term storage locations for working copies are not part of this definition.”

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy support the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Jeremy Voll - Basin Electric Power Cooperative - 3

Answer	No
Document Name	

Comment

Support the MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	

Although the proposed revision explicitly states the requirement to identify specific BCSI storage locations, it does not add any actual new flexibility about designating BCSI storage locations. The same flexibility exists today between the lines of existing CIP-004 and CIP-011. It is just implicit, rather than explicit. The confusion remains about the necessity (or lack thereof) to store BCSI in designated BCSI storage locations, how large a collection of BCSI has to be to warrant a BCSI storage location of its own, or how long BCSI can be in use outside of a storage location without creating security and compliance concerns.

Seattle City Light believes a more effective approach would be to clearly state a security objective (“to prevent unauthorized access to BCSI”), require an entity to develop a risk-informed BCSI security plan to achieve this objective, and then require implementation and periodic review of the BCSI security plan. Beyond this, almost all details about specific approaches for and elements that might be expected in a BCSI security plan should be provided in the measures and/or technical guidelines. A few specific elements of the security plan might be requested as sub-requirements, such as i) how to identify BCSI; ii) controls to limit unauthorized access to BCSI in use, transit, and storage; and iii) security requirements expected of third party that uses and/or stores BCSI for the entity, if an entity chooses to employ such parties. Note that by iii) Seattle does NOT mean that any specific security requirements for third party providers should be spelled out as requirement in the revised Standard, but rather than each entity should develop its own risk-based list of the security controls/requirements it demands of any third party provider it may employ with regard to BCSI. And that such entity-specific control requirements would only be required if an entity elected to use third-party BCSI providers. Guidance as to what these requirements might be could be provided in the Measures or supporting technical document.

If a more prescriptive approach to controls is desired, Seattle shares the same concerns expressed by Sacramento Municipal Utility District (SMUD) regarding the change of language about BCSI storage locations.

Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

‘System Information pertaining to’ in the applicability column may broaden scope expectations and should be removed.

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1

Answer	No
Document Name	

Comment

We support the overall effort. However, we do not support introducing "System information pertaining to" in the applicability section. This creates some ambiguity. We believe that the applicability should be limited to BCSI.

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 draft language in present form would obligate entities to establish a Data Loss Prevention program to fully satisfy this requirement. This doesn’t support the scope or intent of the original SAR. This goes far beyond controlling access to BCSI and includes topic that may cover how an individual may handle that information (replication, forwarding, etc.). The previous version included the term “Designated repository” for identification of scope of protection. Removal of this qualification creates an obligation to manage BCSI regardless of where it may occur.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

As written the requirement may require the Registered Entity (RE) identify the physical locations a third-party provider is storing the RE's BCSI. We think that it would make more sense to identify the access controls and methods the RE has in place controlling the ability to obtain and use the information.

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3

Answer	No
Document Name	

Comment

AEP agrees with EEI's comments and requests clarification on the requirement to identify BES Cyber System Information (BCSI) storage locations as proposed by the Standard Drafting Team (SDT) for CIP-011-3, Requirement R1, Part 1.1. As written, this requirement would require registered entities to work with their third-party cloud-based service providers to identify the physical location where their BCSI resided on the service provider's cloud-based network. This would be difficult (or possibly impractical) for entities to maintain suitable records on an ongoing basis.

Also, from a compliance perspective, registered entities would have difficulty proving that they granted or removed access to BCSI, as required in the proposed draft for CIP-004-7. To resolve this concern, we suggest that the SDT modify the proposal to require registered entities to prove access is granted or removed to a BCSI Repository.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

AECI supports comments filed by NRECA

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

NRECA does not support the replacement of the term “method” with the term “process.” A “method” for identification allows Responsible Entities to provide guidelines and criteria to their personnel to aid in identification of BCSI without requiring a pre-defined series of steps or action (e.g., a process) to be utilized by such personnel in the identification. This distinction is critical because a process can be high-level and – thereby – provide significant variability in what is identified as BCSI whereas a method provides personnel with enough guidance to provide consistency relative to BCSI identification without being overly prescriptive regarding how such identification is accomplished.

Additionally, NRECA does not support the addition of a requirement to “identify applicable BES Cyber System Information storage location.” The Technical Rationale indicates that the SDT wanted to shift focus from the storage location to the information; however, this addition places the focus back on to the storage location for what appears to be solely administrative purposes. As well, the description of what was intended for identification in the Technical Rationale exceeds the scope of the verbiage added to Requirement R1.1. Identification of an object is different than description of an object and the requirement language addresses only the former while the Technical Rationale is clearly suggesting the latter. Thus, this addition creates ambiguity and confusion regarding Responsible Entity’s obligations for little or no benefit to BES reliability.

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

The addition of a new requirement is not necessary because 1) REs already have the flexibility to identify BCSI storage locations, and 2) None of the rest of the proposed requirements reference storage locations anyway.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

GSOC does not support the replacement of the term “method” with the term “process.” A “method” for identification allows Responsible Entities to provide guidelines and criteria to their personnel to aid in identification of BCSI without requiring a pre-defined series of steps or action (e.g., a process)

to be utilized by such personnel in the identification. This distinction is critical because a process can be high-level and – thereby – provide significant variability in what is identified as BCSI whereas a method provides personnel with enough guidance to provide consistency relative to BCSI identification without being overly prescriptive regarding how such identification is accomplished.

Additionally, GSOC does not support the addition of a requirement to "identify applicable BES Cyber System Information storage location." The Technical Rationale indicates that the SDT wanted to shift focus from the storage location to the information; however, this addition places the focus back on to the storage location for what appears to be solely administrative purposes. As well, the description of what was intended for identification in the Technical Rationale exceeds the scope of the verbiage added to Requirement R1.1. Identification of an object is different than description of an object and the requirement language addresses only the former while the Technical Rationale is clearly suggesting the latter. Thus, this addition creates ambiguity and confusion regarding Responsible Entity's obligations for little or no benefit to BES reliability.

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	No
Document Name	

Comment

SMEC agrees with comments submitted by NRECA.

SMEC also disagrees with the removal of the qualifying language "with ERC" from the applicability of Medium Impact BES Cyber Systems in CIP-011-3 R1.1 as currently provided in CIP-004-6 R4.1, and how this greatly and needlessly expands the scope of all subsequent parts of R1, and R2.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

IESO agrees in principle with the comments submitted by NPCC:

1. We recommend security objectives instead of prescriptive requirements. Information protection program should include identification, access control, etc.
2. For the Applicability column referencing "system information," we suggest changing "System information pertaining to:" to "Information associated with," or clarification of what is considered "system information"
3. We recommend clarifying by stipulating that the Entity's information protection plan includes a description of the storage location(s) and that the Entity maintains a list of those storage locations

4. It is unclear if the intent of R1.1. is also for an entity to *develop a process* to list the storage locations or the actual inventory list of the storage locations. If the intention is not a “process”, then subdivide 1.1 requirement into two component parts: 1.1.1 a process to identify what constitutes BCSI and 1.1.2 a second requirement to have an inventory of locations.

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

No, the current version of CIP-004 already provides for the identification of BCSI storage locations. Keeping all the requirements for access and revocation in one standard decreases the complexity for compliance.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

The SDT should consider that with cloud computing the physical location of BCSI is irrelevant. It is more important to protect the data vs where the data is located. Cloud computing currently replicates data in data centers world-wide. Entities will not be able to verify where cloud BCSI exists.

This is duplicative in nature. The requirement to approve access by itself requires entitites to know where the data is located. Hence authorization though roles or entitlments identifies the locations of the BCSI.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	
Comment	

With respect to Applicability, the term 'System Information" is undefined. Perhaps the team intended to include "BES Cyber System Information" In any case, greater clarification of this term is needed.

The term "Method" allows the Registered Entity greater flexibility to provide guidance to meet the intended security objectives of the requirement. In that regard, I do not agree that the use of the term "process" is a better choice for this requirement as this implies a rigid step-by-step structure.

With respect to the Measure concerning "Indications on information.....", the language should be clarified to permit classification of the electronic storage location as contaning BCSI and not each individual document or file while at rest within that access-controlled location. Indications should be considered for data in transit.

I agree that a listing of individual storage locations for BCSI should be identified and maintained.

Likes 0	
Dislikes 0	
Response	

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	
Comment	

New and emerging technologies shift the paradigm of security controls away from a specific storage location/repository to the ability to access and use the information itself. For example, an entity that utilizes file level security can apply encrypted protections on the data that preclude unauthorized access to the data regardless of where it is stored. Requiring a list of storage locations is an antiquated construct that disincentivizes entities from using potentially more secure mechanisms because of the impossibility of compliance with documenting storage locations. The requirement should be technology agnostic and objective based, so it is written to focus on the implementation of effective methods that afford adequate security protections to prevent unauthorized access to the information.

Likes 0	
Dislikes 0	
Response	

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3

Answer	No
Document Name	
Comment	

‘System Information pertaining to’ in the applicability column may broaden scope expectations and should be removed.

Likes 1	Barry Jones, N/A, Jones Barry
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

See NRECA submitted comments.

Likes 1	Barry Jones, N/A, Jones Barry
Dislikes 0	

Response

Anton Vu - Los Angeles Department of Water and Power - 6

Answer	No
Document Name	

Comment

New R1.1 still stresses “Identify applicable BES Cyber System information storage locations.” According to the SAR, the emphasis was supposed to move away from storage “locations” and focus on the protection of the information itself. However, to maintain security of information being stored outside of a Registered Entity using cloud services and vendors, to conform to the SAR, and without imposing undue regulatory burdens to entities using encryption key management for BCSI stored within the Responsible Entity, the language should be modified to say “Identify applicable BES Cyber System information storage locations *not owned or managed by the Responsible Entity.*”

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

Yes, we agree that the language in R1 Part 1.1, as written, allows the Responsible Entity the flexibility in identifying BCSI storage locations.

While the requirement is necessary, we do propose splitting R1 Part 1.1 into two parts as follows:

In Part 1.1: change the Requirement to delete the phrase, “and identify applicable BES Cyber System Information storage locations.” Also, in the Measures, delete last bullet.

Recommend creating a new Part 1.2: with the ‘Applicability’ as Part 1.1, but add, “with ERC” to Medium Impact BES Cyber Systems, and in the Requirement section, “Method(s) to identify applicable BES Cyber System Information storage locations.”

We agree with EEI’s suggestion to create the new term “BCSI Repository” to better define BCSI storage locations.

Applicability of current R1 Parts 1.3 to 1.6, and R2 Parts 2.1 and 2.2, change to reference a newly created R1 Part 1.2.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC	
Answer	No
Document Name	
Comment	
NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES	
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	
Part 1.1 as written requires a process for identifying two things; BCSI and BCSI storage locations. However there is no other mention of BCSI storage locations within the standard. Since there are no proposed requirements for these storage locations, a process to identify them has no function. The remainder of the requirements apply to the BCSI as identified in R1.1 with no further mention of the storage locations. We are concerned with the philosophical shift from BCSI storage locations as the object of many of the requirements to the BCSI itself, in particular all the requirements that were previously in CIP-004. Managing and auditing access to BCSI as simply information in whatever form and wherever it is being used is an infinite scope. In order for access to be managed and audited, it must have finite and discrete objects such as designated BCSI storage locations. For example, entities will be unable to prove compliance with CIP-011 (R1.3 and R1.5 in particular) on BCSI as it exists in the form of a working copy of a printed network diagram used by a technician in a substation to troubleshoot a communications issue. By making BCSI the object of the requirements rather than the designated storage locations, the scope has been expanded to a point that is unmanageable and unmeasurable with which entities are unable to prove compliance. We suggest the object of the requirements remain as they were in CIP-004 and explicitly reference designated BCSI storage locations as their object, not simply BCSI.	

Also, the requirement does not “allow an entity the flexibility” to identify storage locations for BCSI, it requires that an entity do so. The identification of storage locations containing BCSI is, for all practical audit purposes, already required under CIP-011-2 (See the NERC Evidence Request Tool, BCSI Tab), and the proposed wording does not allow any flexibility – it explicitly requires an entity to develop and maintain a list.

The applicability of Part 1.1 has changed to “System information pertaining to…”, which raises a concern over what “system information” is and how does an entity prove they have performed their BCSI identification process on the universe of all such information? We are concerned that “system information” is not a finite or discrete scope for this requirement. A requirement with a stated applicability of all possible information about a system is a showstopper issue.

Southern suggests that instead it should require a process for determining BCSI for high/medium impact BCS. An example replacement R1 that is not in “table format” could state “Each Responsible Entity shall have a process to identify BCSI that pertains to high impact or medium impact BCS and their associated EACMS and PACS.” Subsequent R2, R3, etc. could then outline the necessary parts of the information protection program scoped to that identified BCSI.

If keeping the table format for R1 is desired, retaining the the high/medium impact BCS as the applicability of Part 1.1 and then require “Processes to identify BCSI that pertain to the applicable systems” is preferable. It should stay scoped to high/med impact BCS and not the full universe of system information.

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.

In addition, as an alternative to EEI’s proposed definition for BCSI Repository, SDG&E tenders its alternate definition below:

BCSI Repository – Either a physical or electronic storage location where BES Cyber System Information is stored, and for which access is controlled. For physical BCSI Repositories, this would be a physical location. For electronic BCSI Repositories, this would be a logical location.

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 response found in the NSRF Comment Form	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	

1. We would recommend security objectives (similar to CIP-013-1) instead of prescriptive requirements. Information protection program should include identification, access control, etc.
2. We suggest changing “System information pertaining to:” to “Information associated with,” or clarify the term “system information”.

Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	

Yes, we agree that the language in R1 Part 1.1, as written, allows the Responsible Entity the flexibility in identifying BCSI storage locations.

However, we share the concerns expressed by EEI.

While the requirement is necessary, we do propose splitting R1 Part 1.1 into two parts as follows:

In Part 1.1: change the Requirement to delete the phrase, "and identify applicable BES Cyber System Information storage locations." Also, in the Measures, delete last bullet.

Recommend creating a new Part 1.2: with the 'Applicability' as Part 1.1, but add, "with ERC" to Medium Impact BES Cyber Systems, and in the Requirement section, "Method(s) to identify applicable BES Cyber System Information storage locations." This could in turn be changed to "Method(s) to identify applicable BES Cyber System Information Repositories" per the EEI recommendations.

We agree with EEI's suggestion to create the new term "BCSI Repository" to better define BCSI storage locations.

Applicability of current R1 Parts 1.3 to 1.6, and R2 Parts 2.1 and 2.2, change to reference a newly created R1 Part 1.2.

Likes 0	
Dislikes 0	

Response

Ayman Samaan - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

Our first suggestion is that the Applicability for 1.1 be returned to it's original state without any additional conditions or prerequites. Absent that,

1. We recommend security objectives instead of prescriptive requirements. Information protection program should include identification, access control, etc.

2. Since we have some debate over “system information,” we suggest changing “System information pertaining to:” to “Information associated with,” or clarification of “system information”. At a minimum, if “system information” must be used. It should be established as a NERC glossary Defined Term.

3. We recommend clarifying by stipulating that the Entity’s plan includes a description of the storage location(s) and maintains a list of those storage locations.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	No
Document Name	

Comment

The SAR stressed that changes would be focused on “…BCSI and the ability to obtain and make use of it”, where the current standard “…focused on access to the ‘storage location’…”, yet the proposed changes add additional requirements to identify the storage locations. This seems to be contrary to the main objective of the SAR. We have additional concerns about what the SDT means about storage location and how it pertains to storage at vendors and their networks. We suggest that the SDT clarify what their intent was regarding the changed requirement on storage location.

Additionally, the proposed changes add PCAs as applicable systems, which by definition do not contain BCSI. It seems that this addition is outside of the SAR and it would be helpful for the SDT to describe how adding this “clarifies the protections expected when utilizing third-party solutions”. We believe that no changes are needed to R1 Part 1.1 to address the SAR and thus, the current language should remain the same.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support MRO comments.

Likes 0	
Dislikes 0	

Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	

Comments: MISO agrees the changes are necessary; however, we also have concerns. As the existing language in CIP-004-6, requirement R4, part 4.1.3 implies and/or can be interpreted as limiting access to the storage location as opposed to controlling access to BCSI regardless of location, MISO supports adding language to require identifying information and applicable BCSI storage locations will expand flexibility and options.

That said, MISO proposes the SDT more clearly articulate the following key distinctions raised during the Q&A portion of the 2019-02: BES Cyber System Information Access Management Webinar hosted on January 16, 2020: physical or electronic, responsible entity or vendor hosted. To make this clear in the proposed standard, MISO proposes the SDT expand the language of the last example provided under requirement R1, Part 1.1, Measures as follows:

"Storage locations *(physical or electronic, responsible entity or vendor hosted)* identified for housing BES Cyber System Information in the entity's information protection program"

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) supports the comments as submitted by the Edison Electric Institute.

Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

EEI member companies (EEI) identified four issues for further consideration by the SDT and proposes solutions to address some of those issues.

First, EEI urges the SDT to clarify the requirement to identify BES Cyber System Information (BCSI) storage locations as proposed by the SDT for CIP-011-3, Requirement R1, Part 1.1. The requirement, as written, requires registered entities to work with their third-party cloud-based service providers to identify the physical location where their BCSI resided on the service provider's cloud-based network. The challenge is the difficulty and, potential impracticality for entities to track down and maintain records from service providers to demonstrate compliance on a continuing basis. To address this challenge, the SDT should clarify BCSI "Storage Location" and address electronic and physical repositories within that definition. As an alternative, EEI suggests the SDT define the term "BCSI Repository," which would provide registered entities a simpler solution than what was provided in the proposed revisions to CIP-004-7 and CIP-011-3. Additionally, EEI offers the following definition for SDT review and consideration:

BCSI Repository – Either a physical or electronic storage location where BES Cyber System Information is retained. For physical BCSI Repositories, this would be a physical location. For electronic BCSI Repositories, this would be a logical location. **Notes:** *Issues surrounding short term storage of BCSI (e.g., working copies, etc.) are not intended to be part of this definition but would need to be addressed by responsible entity's policies and procedures.*

Second, to provide clarity with respect to the applicability of Requirement R1, Part 1.1., EEI suggests replacing the undefined term, "system information" with the NERC defined term, "BES Cyber System Information."

Third, the SDT's proposal creates compliance challenges. Registered entities would have difficulty proving the granting and removal of access to BCSI as contemplated in the proposed draft for CIP-004-7. As an alternative, EEI suggests using the BCSI Repository definition shown above, and revising proposed CIP-004-7 to require registered entities to prove access and removal of access to a BCSI Repository.

Fourth, EEI is concerned that the SAR scope may have expanded without providing necessary justification within the Technical Rationale. See our comments to Questions 11 below.

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2

Answer	No
Document Name	

Comment

NYISO felt that the changes are necessary. The existing language in CIP-004-6, requirement R4, part 4.1.3 implies and/or can be interpreted as limiting access to storage location options as opposed to controlling access to BCSI regardless of location. By adding language to require identifying information coupled with an identification of applicable BCSI storage locations would certainly add acceptable options and provide a responsible entity flexibility in choosing technology solutions.

In addition, NYISO feels that the SDT more clearly articulated key distinctions during the Q&A portion of the 2019-02: BES Cyber System Information Access Management Webinar that was hosted on January 16, 2020. In order to make this clearer, NYISO would suggest that the SDT should endeavor to expand the language of the last example in the current draft provided under requirement R1, Part 1.1, Measures as follows:

"An inventory of locations, either physical or electronic, either housed within a responsible entity's data center or vendor hosted that are identified as housing the responsible entity's BES Cyber System Information be a part of the entity's information protection program"

Likes 0	

Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NextEra	
Answer	No
Document Name	

Comment
1) We recommend security objectives instead of prescriptive requirements. Information protection program should include identification, access control, etc. 2) Since we have some debate over “system information,” we suggest changing “System information pertaining to:” to “Information associated with,” or clarification of “system information”. 3) We recommend clarifying by stipulating that the Entity’s plan includes a description of the storage location(s) and maintains a list of those storage locations.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	

Comment
The requirement is not necessary. Why should we have to identify our locations to NERC? There should be security objectives instead of prescriptive requirements.

Likes 0	
Dislikes 0	

Response

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	

Comment

SNPD is concerned that the proposed wording INCREASES rather than DECREASES ambiguity. The current language is understood to require Entities to designate BCSI storage locations, which is the fundamental security imperative to enable proper access control. Semantics between terms such as “designate” vs. “identify” or another synonym will not fundamentally alter how Entities choose to interpret and respond to R1. There are already substantial differences between how Entities interpret the current language. In other words, the current wording is descriptive and defines the imperative.

Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	

Response

Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF

Answer	No
Document Name	

Comment

Alliant Energy agrees with NSRF and EEI’s comments.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG is in agreement with RSC provided comment

Likes 0	
Dislikes 0	

Response

James Brown - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

The approach of identifying the storage locations is welcomed since this is where controls are applied and is compatible to current CIP-004 requirements. The drafting team needs to avoid requirements that can be interpreted as requiring protection of each individual piece of BCSI.

It would be helpful to clearly define what is meant by “storage locations”. Is it geographical? Is it the server or tenant with a cloud provider? This distinction could be important when BCSI is housed by a vendor or other third-party. Consider adding identification of a) storage locations with the entity, b) with a vendor who provides custom services with identified personnel for in scope cyber systems or assets and c) with a certified cloud service provider who provides generic cloud based services without insider knowledge.

The Applicability column needs to be modified to limit the information to only BCSI, and not all system information pertaining to the system categories listed. Just using “system information” will cast too wide of a net on identifying BCSI. Consider revising as, “BES Cyber System Information for:” This is easily understood since it is a defined term with defined criteria.

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2

Answer	No
Document Name	

Comment

PGE agrees with EEI’s comments

Likes 1	Portland General Electric Co., 3, Zollner Dan
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

No, The term “designated storage locations” offered additional clarity that it was only those storage locations designated as such by the responsible entity that would meet this requirement. However, the updated term “applicable BES Cyber System Information storage locations” offers no clarity of

which storage locations would be applicable. This could have the unintended consequence of increasing the scope of locations to be managed under CIP. The term is too broad, and should be left as “designated storage locations” or amended to “designated storage locations of BCSI.”	
Likes 0	
Dislikes 0	
Response	
Angela Gaines - Portland General Electric Co. - 1	
Answer	No
Document Name	
Comment	
Please see comments PGE Group 2	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
The requirement is not necessary. Why should we have to identify our locations to NERC? There should be security objectives instead of prescriptive requirements.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
Yes, we agree that the language in R1 Part 1.1, as written, allows the Responsible Entity the flexibility in identifying BCSI storage locations.	

However, we share the concerns expressed by EEI and the MRO NSRF.

While the requirement is necessary, we do propose splitting R1 Part 1.1 into two parts as follows:

In Part 1.1: change the Requirement to delete the phrase, “and identify applicable BES Cyber System Information storage locations.” Also, in the Measures, delete last bullet.

Recommend creating a new Part 1.2: with the ‘Applicability’ as Part 1.1, but add, “with ERC” to Medium Impact BES Cyber Systems, and in the Requirement section, “Method(s) to identify applicable BES Cyber System Information storage locations.” This could in turn be changed to “Method(s) to identify applicable BES Cyber System Information Repositories” per the EEI and MRO NSRF recommendations.

Applicability of current R1 Parts 1.3 to 1.6, and R2 Parts 2.1 and 2.2, change to reference a newly created R1 Part 1.2.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The approach of identifying the storage locations is welcomed because this is where controls are applied, and the approach is compatible to current CIP-004 requirements. ERCOT suggests the drafting team avoid requirements that can be interpreted as requiring protection of each individual piece of BCSI.

ERCOT believes it would be helpful to clearly define what is meant by “storage locations.” Is it geographical? Is it the server or tenant with a cloud provider? This distinction could be important when BCSI is housed by a vendor or other third-party. ERCOT suggests the drafting team consider adding identification of (a) storage locations with the entity, (b) vendors that provide custom services with identified personnel for in scope cyber systems or assets, and (c) certified cloud service providers that provide generic cloud based services without insider knowledge.

The Applicability column should be modified to limit the information to only BCSI, and not all system information pertaining to the system categories listed. Just using “system information” may cast too wide of a net on identifying BCSI. ERCOT suggests the drafting team consider revising to read “BES Cyber System Information for:” This would likely be more easily understood because it is a defined term with defined criteria.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1,

3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, 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 does not agree with required identification of BCSI storage locations. The stated purpose and emphasis of the modifications is the protection of “System Information” (i.e. BCSI) and PGAE does not believe that this burdensome requirement enhances protection of BCSI. The requirement to identify storage locations has been administratively burdensome and challenging for BCSI placed on internal servers but could be impossible for BCSI placed on third-party provider infrastructure (i.e. cloud), especially if the service providers have the capability to store the BCSI on multiple instances of their infrastructure for redundancy and resilience. PG&E recommends the required identification of storage locations be removed while maintaining the emphasis on the protection of the BCSI.	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No
Document Name	
Comment	
The change from "designated storage locations" to "applicable ... storage locations" increases the confusion that already surrounds this topic.	
Likes 0	

Dislikes 0	

Response

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

Comment
Yes, we agree that the language in R1 Part 1.1, as written, allows the Responsible Entity the flexibility in identifying BCSI storage locations. However, we share the concerns expressed by EEI and the MRO NSRF. While the requirement is necessary, we do propose splitting R1 Part 1.1 into two parts as follows: In Part 1.1: change the Requirement to delete the phrase, “and identify applicable BES Cyber System Information storage locations.” Also, in the Measures, delete last bullet. Recommend creating a new Part 1.2: with the ‘Applicability’ as Part 1.1, but add, “with ERC” to Medium Impact BES Cyber Systems, and in the Requirement section, “Method(s) to identify applicable BES Cyber System Information storage locations.” This could in turn be changed to “Method(s) to identify applicable BES Cyber System Information Repositories” per the EEI and MRO NSRF recommendations. Applicability of current R1 Parts 1.3 to 1.6, and R2 Parts 2.1 and 2.2, change to reference a newly created R1 Part 1.2

Likes 0	
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	

Comment
We recommend clarifying the requirement by stipulating that the Entity’s plan includes a description of the storage locations for BCSI and maintains a list of those storage locations. In addition, there should be language describing what is meant by “storage locations.” The definition is important when

BCSI is housed by a vendor or other third-party. Finally, the requirement should cover only BCSI and not all system information pertaining to the system categories listed in the Applicability column. Accordingly, “system information” in the Applicability column should be changed to the defined term “BES Cyber System Information.”	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
In its current form, CIP-004 and CIP-011 already provides flexibility. The current requirements to address access to sensitive data and information seem acceptable in the current formats. What is unclear is how the BCSI will be usable if it must always reside in specific locations? For example, is it violation if someone who has access, temporary pulls that information off the stored location and prints the document for review? While a copy of that data is stored in the storage location, the hard copy now creates an issue. What happens when that person takes it outside the physical security perimeter? Entities should be required to describe how they identify BCSI, how BCSI is transmitted, whom may have access to the data and information, the description electronic access controls, and how exceptions, if any, exist in relation to the use of the information outside of those parameters. The real issue is where it is stored. Auto saves, inadvertent machine shutdowns, etc. may cause the data to be stored in a location outside the acceptable storage location. Virtualization, Office 365, etc. may cause issues for entities to be able to ensure the information is never stored outside of a set storage location. While SunPower believes there can be adequate controls, the programs and systems industry use will likely cause an increase of possible violations as those programs and systems change by the provider. Temporary storage on local devices that are also secured by an approved user should be allowed, at least on a temporary basis.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
While the requirement seems flexible, it is subject to confusion in implementation. The previous version specificially identified electronic or physical controls. This version extends scope to include the cloud. However, in doing so, it removes the context for full understanding of the requirement. Lacking this context, there is a signficant potential of having multiple interpretations of the requirement.	
Likes 1	Miller Scott On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1;
Dislikes 0	
Response	
William Hutchison - Southern Illinois Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Comments: We feel the language could be clearer if the BES Cyber System itself was excluded being it is already being protected by the NERC CIP requirements. The same problem exists within the standard today. It does not exclude BCSI contained within the BES Cyber System itself. Although it is inherent BES Cyber Systems contain BCSI, the standards do not exclude those systems/Cyber Assets from containing BCSI, thus the Cyber Assets themselves would be BCSI repositories and should be documented as such. We have not seen this as a problem in audit, but a strict auditor could make this an issue the way it is written. Also, examples of potential Cyber Assets containing BCSI could be better expanded in the Guidelines and Technical Basis, such as SIEMs, Anti-virus servers, backup servers, etc. which are not a part of a BES Cyber System and the rationale behind why they are or are not considered BCSI repositories.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	

Duke Energy generally agrees that CIP-011-3 R1, Part 1.1 allows flexibility to identify which storage locations are for BCSI and agree the requirement is necessary.

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

While we agree that including the need to identify storage locations, this could prove burdensome to entities. Identification of a location in cloud storage providers (e.g. OneDrive, Microsoft Teams, Sharepoint, etc.) which offer seamless creation and storage of documentation may make it difficult to identify specific storage locations. This could result in entities not listing key storage locations or generalizing, at a loss of security, in order to meet the requirement.

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller

Answer	Yes
Document Name	

Comment

There is more than one question and we vote yes on the first question and no on the second. There should only be one quetion, not two.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Yes, due to improved applicability and exclusion of low impact assets.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	Yes
Document Name	

Comment

Agree with adding requirement to identify BCSI storage locations even though it is already

Implicitly required to be identified in CIP-004-6 R4.1. To better identify BCSI storage locations, we

would suggest making a definition of BCSI Repository as follows:

“A multi-user electronic or physical locations where a collection of BCSI is retained for long-term

storage.”

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

We feel the language could be clearer if the BES Cyber System itself was excluded being it is already being protected by the NERC CIP requirements. The same problem exists within the standard today. It does not exclude BCSI contained within the BES Cyber System itself. Although it is inherent BES Cyber Systems contain BCSI, the standards do not exclude those systems/Cyber Assets from containing BCSI, thus the Cyber Assets themselves would be BCSI repositories and should be documented as such. We have not seen this as a problem in audit, but a strict auditor could make this an issue the way it is written.

Also, examples of potential Cyber Assets containing BCSI could be better expanded in the Guidelines and Technical Basis, such as SIEMs, Anti-virus servers, backup servers, etc. which are not a part of a BES Cyber System and the rationale behind why they are or are not considered BCSI repositories.

Likes 0	

Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
N&ST suggests changing: “Process(es) to identify information that meets the definition of BES Cyber System Information and identify applicable BES Cyber System Information storage locations” to “Process(es) to identify information that meets the definition of BES Cyber System Information and to identify BES Cyber System Information storage locations.”	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE recommends revising “System information” to “Information” in the Applicability column to be consistent with the Requirement language.	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	

Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
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	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Vivian Moser - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
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	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
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	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 1	BC Hydro and Power Authority, 5, Hamilton Harding Helen
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Colleen Campbell - AES - Indianapolis Power and Light Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 1	NiSource - Northern Indiana Public Service Co., 3, Bazylyuk Dmitriy
Dislikes 0	
Response	

2. The standard drafting team (SDT) attempted to maintain backwards compatibility with concepts of designated storage locations and access-level requirements previously contained in CIP-004-6. Do you agree that there is a minimal effort to meet this objective while providing greater clarity between BCSI and BES Cyber System (BCS) requirement obligations?

Bradley Collard - SunPower - 5

Answer	No
Document Name	

Comment

It appears the scope has greatly expanded. Because of the focus of all possible BCSI storage locations, entities will not only be focused on who should have access and how access is controlled, but where that information may be stored temporally and where it might be duplicated.

Additionally, how are Cloud storage services handled in the new CIP-011-3? The physical security perimeter of that service exists outside of the control of the registered entity.

If, during a CIP Exceptional Circumstance, information is transmitted to another person to help facilitate an issue, at the end of the CIP Exceptional Circumstance, data cleanup becomes a problem.

Are entities to identify the RE file server location if an entity is required to send a Regional Entity BCSI?

The focus should be access controls, as the long-term storage is already considered in that process.

Likes 0	
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2

Answer	No
Document Name	

Comment

Comments: No. The CIP-004-6 requirements are based on an “Applicable System” approach and access to BCSI designated electronic and physical storage locations. However, CIP-011 shifts the paradigm to “Applicability,” access to BCSI, and the ability to obtain and use the information.

Recommendation: Ensure that the implementation timeline accounts for the need to shift the construct of an Entity’s information protection program.

Likes 0	
Dislikes 0	

Response

Colleen Campbell - AES - Indianapolis Power and Light Co. - 3

Answer	No
Document Name	

Comment

By moving the requirements from CIP-004 to CIP-011 will require a reworking of existing evidence and will cause confusion during any subsequent audits.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

We support the EEI and MRO NSRF comments that disagree with the qualifying language “with ERC” dropping from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 when moved to CIP-011-3 R1.3. This deletion greatly expands the scope of this requirement, and may have created a situation where Responsible Entities could be subject to multiple compliance violations based on a single action due to overlapping obligatations in the CIP Standards.

Having a lack of ERC also renders BCSI pertaining to Medium Impact BES Cyber Systems outside the scope of R1 Part 1.2, as such information, if obtained, cannot be used remotely, as there is no remote access to the Cyber Systems. Information pertaining to these Cyber Systems can only be used to compromise them by breaching physical security.

There also is significant scope expansion with the authorization/revocation and review requirements now applying to all BCSI (not just designated storage locations of BCSI). This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a considerable protection.

Likes 0	
Dislikes 0	

Response

Allan Long - Memphis Light, Gas and Water Division - 1

Answer	No
Document Name	

Comment

"Method(s) to prevent the unauthorized access to and use of BES Cyber System Informatin during storage, transit, use, and disposal." is a practical than "elminate the ability to ...."

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

We support the EEI and MRO NSRF comments that disagree with the qualifying language “with ERC” dropping from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 when moved to CIP-011-3 R1.3. This deletion greatly expands the scope of this requirement, and may have created a situation where Responsible Entities could be subject to multiple compliance violations based on a single action due to overlapping obligatations in the CIP Standards.

Having a lack of ERC also renders BCSI pertaining to Medium Impact BES Cyber Systems outside the scope of R1 Part 1.2, as such information, if obtained, cannot be used remotely, as there is no remote access to the Cyber Systems. Information pertaining to these Cyber Systems can only be used to compromise them by breaching physical security.

There also is significant scope expansion with the authorization/revocation and review requirements now applying to all BCSI (not just designated storage locations of BCSI). This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a considerable protection.

Likes 0	

Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
I don't see backwards compatibility based on the methods listed in 1.2.	
Likes 0	
Dislikes 0	
Response	
Angela Gaines - Portland General Electric Co. - 1	
Answer	No
Document Name	
Comment	
Please see comments PGE Group 2	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	No
Document Name	
Comment	
No, The term “designated storage locations” offered additional clarity that it was only those storage locations designated as such by the responsible entity that would meet this requirement. However, the updated term “applicable BES Cyber System Information storage locations” offers no clarity of which storage locations would be applicable. This could have the unintended consequence of increasing the scope of locations to be managed under CIP. The term is too broad, and should be left as “designated storage locations” or amended to “designated storage locations of BCSI.”	

Additionally, the CIP-004-6 access level requirements were scoped to High Impact BCS, and Medium Impact BCS with ERC. The CIP-011 replacement broadly expands the scope of the access level requirements.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE agrees with EEI's comments	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	No
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
All BCSI access requirements should remain under CIP-004 as one Standardized Security Standard (centralized location). Leaving the BCSI access with cyber and physical provides a holistic security access management and review program verses fragmenting access management.	

Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
SNPD is concerned that the proposed wording INCREASES rather than DECREASES ambiguity. The current language is understood to require Entities to designate BCSI storage locations, which is the fundamental security imperative to enable proper access control. Semantics between terms such as "designate" vs. "indentify" or another synonym will not fundamentally alter how Entities choose to interpret and respond to R1. There are already substantial differences between how Entities interpret the current language. In other words, the current wording is descriptive and defines the imperative.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
I don't see backwards compatibility based on the methods listed in 1.2.	

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2

Answer	No
Document Name	

Comment

NYISO's response is based on the assumption this question relates to the proposed changes in CIP-011-3 within requirement R1, parts 1.3, 1.5 and 1.6.

NYISO believes that the proposed changes maintain backwards capability. That said, the proposed changes in CIP-011-3 also introduce a potential complication; having to maintain similar access authorization, revocation and control measures as that currently contained within CIP-004-7. This could create a situation whereby a single deficiency in an entity's access management program could lead to potential non-compliance with two separate NERC standards.

Note – during the Q&A portion of the 2019-02: BES Cyber System Information Access Management Webinar hosted on January 16, 2020*, the SDT explained that their intent in proposing these modifications was to direct the content of CIP-004-7 solely on BCS while focusing the content of CIP-011-3 solely on BCSI.*

NYISO recognizes and agrees with the SDT's intent to consolidate similar issues. Our recommendation would be for the SDT to maintain all personnel and access management requirements within CIP-004-7 to better align with existing industry practices. In addition, NYISO would also propose that the SDT consider similar treatment of vendor related risk assessment requirements be incorporated and consolidated within CIP-013-2.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

EEI appreciates the considerable efforts of the SDT to streamline Requirements associated with BCSI within the proposed changes to CIP-004-7 and CIP-011-3. However, EEI is concerned that the proposed changes may create a situation where responsible entities could be subject to multiple compliance violations based on a single action due to overlapping obligations in the CIP Standards. For example, if an entity developed a process to remove access to BCSI, including other logical access, and there was a failure in that process, the proposed requirement could be interpreted as a violation of CIP-004-7 R5 and CIP-011-3 R1. Whereas, under the current approved standards this situation would result in a single violation of CIP-004-6 R5.

Likes 0	

Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CEHE does not agree that there is a minimal effort to meet the proposed obligations due to the addition of PCAs. Adding the phrase, “System information pertaining to:” in the Aplicability column does provide greater clarity between BCSI and BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
MISO’s response assumes this question relates to the proposed changes in CIP-011-3, requirement R1, parts 1.3, 1.5 and 1.6. MISO believes the proposed changes maintain backwards capability; however, the proposed changes in CIP-011-3 also introduce a new complication, that of having to maintain similar access authorization, revocation and control measures as that in CIP-004-7. This could create a situation whereby a single deficiency in an entity’s access management program could lead to potential non-compliance with two NERC standards at the same time. *Note – during the* Q&A portion of the 2019-02: BES Cyber System Information Access Management Webinar hosted on January 16, 2020*, the SDT explained their intent in proposing these modifications is to focus the content of CIP-004-7 solely on BCS and the content of CIP-011-3 solely on BCSI.* MISO recognizes and agrees with the SDT’s intent to consolidate similar issues. We recommend that the SDT maintain all personnel and access management requirements within CIP-004-7 to better align with existing industry practices. Likewise, MISO would propose the SDT consider similar treatment of vendor related requirements by incorporating them into CIP-013-2.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No

Document Name	
Comment	
The standards development team should support specific requirements providing appropriate levels of security for Cloud Service Providers and 3rd Party Access. Transferring the CIP-004 BCSI requirements to CIP-011 does not address the unique issues created by storing BCSI in repositories that are not controlled by registered entities. The standards development team should draft separate requirements.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support MRO comments.	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
While we understand the reasoning behind including access to BES Cyber System Information storage locations in CIP-011, the 2016-02 SDT made great efforts to consolidate like requirements together and remove the “spaghetti” requirements. We believe that these changes are undoing that effort. The ability for an entity to have a single access management program (dealing with physical, electronic and information access) provides economy of scale and less opportunities for mistakes or confusion. While we do believe these changes maintain backwards compatibility, we cannot support splitting access management into multiple Standards.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	

Answer	No
Document Name	
Comment	
NYPA believes that some backward compatibility has been lost since the modified Standard has been modified to extend to ALL Medium Impact BES Cyber Systems	
Likes 0	
Dislikes 0	
Response	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We support the EEI comments that disagree with the qualifying language "with ERC" dropping from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 R4.1 when moved to CIP-011-3 R1.3. This deletion greatly expands the scope of this requirement, and may have created a situation where Responsible Entities could be subject to multiple compliance violations based on a single action due to overlapping obligatations in the CIP Standards. *Having a lack of ERC also renders BCSI pertaining to Medium Impact BES Cyber Systems outside the scope of R1 Part 1.2, as such information, if obtained, cannot be used remotely, as there is no remote access to the Cyber Systems. Information pertaining to these Cyber Systems can only be used to compromise them by breaching physical security, in which case the CIP-011 standard provides no protection.*	

There also is significant scope expansion with the authorization/revocation and review requirements now applying to all BCSI (not just designated storage locations of BCSI). This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a sufficient protection.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
We do appreciate the SDT concern with backwards compatibity, but since we are recommending changes to the current drafts of CIP-004-7 and CIP-011-3, we are not able to agree at this time.	
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 response found in the NSRF Comment Form	
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.

SDG&E would like to additionally speak to the new draft standard R1.3 requirement of "Process(es) to authorize access to BES Cyber System Information…" The existing requirements require authorization for the repositories that BCSI is stored in. A change to authorizing access to BCSI generally will be a large deviation from current practices and creates many questions about how to authorize/track access to each piece of BCSI.

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

We do not agree as one of the fundamental concepts of CIP-004 R4 Part 4.1.3 that was lost in the proposed transition to CIP-011 R1 Part 1.3 is the difference between authorizing access to *BCSI storage locations,* which is a discrete and finite object that can be monitored and audited (the current CIP-004 approach), while the new CIP-011 approach is *access to BCSI* wherever and however it exists inside or outside of its storage locations (i.e. a hardcopy of a network diagram in a company truck). This fundamental change has made the requirement unmeasurable and non-auditable. We believe the primary issue of hardware or device level requirements that prevented the use of cloud services was in CIP-011 R2 that required data destruction at a Cyber Asset/physical storage media level. We do not agree with moving the authorization programs away from BCSI *storage locations*. A "storage location" can be a designated encrypted area on a cloud service.

Additionally, we do not agree with moving the "access management" requirements for BCSI out of CIP-004-6 and into CIP-011-3. Although one argument is to keep all requirements applicable to BCSI in a single standard, the same argument could be applied to keep all "access management" requirements in the same standard. This is additionally supported by the fact that this is how all entities have currently structured their compliance programs, and the justification to reallocate those requirements to CIP-011-3 causes more undue burden than any resultant benefit.

Likes 0	
Dislikes 0	

Response

Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC

Answer	No
Document Name	

Comment

NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES

Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes this is not a minimal effort. There is a difference between access to a location and consuming information stored in that location. The need to know standard is not contained in the verbiage of the requirement, but is in the guidance. Need to know implies consuming the information while need to access is simply controlling access. The need to know standard for actually consuming and using information is an unsustainable burden at remote, especially rarely occupied, locations and could interfere with the ability to perform operations in an emergent situation. All personnel with access to storage locations have authorization; those who do not actually consume and use that information nonetheless have a business need to	

access the location. This covers the risk while keeping the burden minimal. A more sustainable objective would be to ensure that all personnel with access are authorized rather than a strict need to know standard. Strict need to know implies compartmentalization that is not sustainable for large organizations with the need to deploy technicians across multiple districts. The language proposed so far would be sustainable if all information were stored electronically and cryptographically protected but this proposes a problem for hard copies stored in substations.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We disagree with the qualifying language “with ERC” dropping from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 R4.1 when moved to CIP-011-3 R1.3. This deletion greatly expands the scope of this requirement, and may have created a situation where Responsible Entities could be subject to multiple compliance violations based on a single action due to overlapping obligatations in the CIP Standards.

Having a lack of ERC also renders BCSI pertaining to Medium Impact BES Cyber Systems outside the scope of R1 Part 1.2, as such information, if obtained, cannot be used remotely, as there is no remote access to the Cyber Systems. Information pertaining to these Cyber Systems can only be used to compromise them by breaching physical security, in which case the CIP-011 standard provides no protection.

There also is significant scope expansion with the authorization/revocation and review requirements now applying to all BCSI (not just designated storage locations of BCSI). This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a sufficient protection.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST sees no benefit in moving BCSI storage location access management requirements from CIP-004 to CIP-011, and believes there is no need for clarification between BCSI and BCS requirements. Furthermore, N&ST believes that the impact of moving some access management requirements

from CIP-004 to CIP-011 could be significant for some Responsible Entities, compelling needless modification and disruption of mature and effective CIP compliance programs.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

See NRECA submitted comments.

Likes 0	
Dislikes 0	

Response

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3

Answer	No
Document Name	

Comment

Tri-State is generally ok with the movement of the requirements from CIP-004 to CIP-011. However, we do not agree with several of the changes.

1) We do not agree with the addition of PCAs to the scope. Furthermore, this was not in scope of the SAR to address.

2) As for R1.2, we think the original language was correct and the concept of “obtain and use” should instead be incorporated into the access requirements, especially R1.3. This will make it clear that in order for someone to be deemed to have access to BCSI, they must have the ability to obtain and use it, which would align with the ERO Practice Guide. Although, we don’t recommend using the term “use” without providing more clarification as to its meaning.

3) Also as it relates to R1.2, we do not agree with the addition of “disposal”. While this is certainly a good security practice, adding this as a compliance requirement would be overly burdensome and unnecessary. Furthermore, this was not in scope of the SAR to address.

4) We think the modifications made to R3 are more prescriptive than the prior version in how to prevent unauthorized retrieval of BCSI and unnecessarily limits the entity’s options in how to meet the security objective. This should be reverted back to previous objective-based language. Furthermore, this was not in scope of the SAR to address.

Likes 0	
Dislikes 0	

Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
New and emerging technologies shift the paradigm of security controls away from a specific storage location/repository to the ability to access and use the information itself. For example, an entity that utilizes file level security can apply encrypted protections on the data that preclude unauthorized access to the data regardless of where it is stored. Requiring a list of storage locations is an antiquated construct that disincentivizes entities from using potentially more secure mechanisms because of the impossibility of compliance with documenting storage locations. The requirement should be technology agnostic and objective based, so it is written to focus on the implementation of effective methods that afford adequate security protections to prevent unauthorized access to the information	
Likes 0	
Dislikes 0	
Response	
Vivian Moser - APS - Arizona Public Service Co. - 3	
Answer	No
Document Name	
Comment	
Although AZPS agrees that meeting this objective likely requires minimal effort, AZPS recommends the SDT address the concept of designated storage locations throughout the Standard. Part 1.1 requires the identification of BCSI storage locations; however, subsequent Requirements omit references to storage locations and instead refer only to the protection of BCSI. The switch from storage locations to BCSI causes confusion and may create challenges in executing the required access management and protection controls.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	

CIP-004 is the appropriate place to require applicable levels of approval prior to granting access to BCSI. Removing the language from CIP-004 and adding it to CIP-011 creates two separate standards that cover access controls in place to protect the Bulk Electic System Information. CIP-011 defines what consititues BCSI and the requirements to protect it. It should not be an standard for approval, auditing and access monitoring.

Secondly, entities will be required to make major changes to their internal governance and compliance program procedures, policies and documentation in order to meet this requirement. Please do not mix standards/requirements

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

The change made to CIP-011-3 Part 1.2 does not add clarity. The choice of the second “use” in Part 1.2 is confusing and does not make sense; “…by eliminating the ability to obtain and use BES Cyber System Information during, storage, transit, use, and disposal.” The SDT needs to elaborate on “…eliminating the ability…” What constitutes elimination of ability?

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	No
Document Name	

Comment

SMEC agrees with comments submitted by NRECA.

SMEC also disagrees with the removal of the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems in CIP-011-3 R1.1 as currently provided in CIP-004-6 R4.1, and how this greatly and needlessly expands the scope of all subsequent parts of R1, and R2

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

GSOC appreciates the SDT's consideration of the important concept of backwards compatibility; however, giving due consideration to the proposed scope expansion to include PCAs; the shift from access authorization to BCSI generally and not storage locations; the shift from methods to processes; and the incorporation of vendor risk assessments and required mitigations into the proposed requirements, GSOC cannot agree that the proposed requirements are actually backwards compatible nor that minimal effort will be required to meet these new requirements.

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	

No, not as proposed.

There is a difference between authorizing access and provisioning access. Per CIP-004-6 Rationale for Requirement R4:

"Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6.

"Provisioning" should be considered the actions to provide access to an individual.

The scope of CIP-004 could be maintained while also changing the focus to the BCSI itself to meet the goals of the SAR by slightly modifying CIP-004 applicable requirement parts to "access to BES Cyber System Information in designated storage locations", such as in part 4.1.3:

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

4.1.3 Access to BES Cyber System Information in designated storage locations.

CIP-004 R4.4 and R5.3 refer to **provisioned access**, and could be modified to include this language as well. For example:

R4.4 Verify at least once every 15 calendar months that provisioned access to BES Cyber System Information in designated storage locations is authorized and implemented correctly.

R5.3 For termination actions, revoke the individual's provisioned access to BES Cyber System Information in designated storage locations by the end of the next calendar day following the effective date of the termination action.

Likes 0	
Dislikes 0	

Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
NRECA appreciates the SDT's consideration of the important concept of backwards compatibility; however, giving due consideration to the proposed scope expansion to include PCAs; the shift from access authorization to BCSI generally and not storage locations; the shift from methods to processes; and the incorporation of vendor risk assessments and required mitigations into the proposed requirements, NRECA does not agree that the proposed requirements are actually backwards compatible nor that minimal effort will be required to meet these new requirements.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI supports comments filed by NRECA	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3	
Answer	No
Document Name	
Comment	
While AEP is appreciative of the SDT's efforts to consolidate BCSI requirements into CIP-011, we do not feel there is minimal effort involved in ensuring compliance. Moving these requirements to a different standard creates more challenges that those who are responsible for complying are required to overcome, leading to more overall work and effort for those involved.	
Likes 0	

Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Black Hills would be in favor of seeing less perscriptive models of access and termination requirements. Additionally, the failure to remove BCSI per CIP-011 could potentially create a scenario where CIP-004's requirements were also unmet, creating a double violation.	
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 removal of the term "designated" greatly expands the scope to cover handling BCSI, including creating replicated copies of applicable BCSI, and ensuring applicable processes and controls are applied to new identified locations / instances of BSCI.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State is generally ok with the movement of the requirements from CIP-004 to CIP-011. However, we do not agree with several of the changes. 1) Tri-State does not agree with the addition of PCAs to the scope. Furthermore, this was not in scope of the SAR to address. 2) As for R1.2, we think the original language was correct and the concept of "obtain and use" should instead be incorporated into the access requirements, especially R1.3. This will make it clear that in order for someone to be deemed to have access to BCSI, they must have the ability to	

obtain and use it, which would align with the ERO Practice Guide. Although, we don't recommend using the term "use" without providing more clarification as to its meaning.

3) Also as it relates to R1.2, we do not agree with the addition of "disposal". While this is certainly a good security practice, adding this as a compliance requirement would be overly burdensome and unnecessary. Furthermore, this was not in scope of the SAR to address.

4) We think the modifications made to R3 are more prescriptive than the prior version in how to prevent unauthorized retrieval of BCSI and unnecessarily limits the entity's options in how to meet the security objective. This should be reverted back to previous objective-based language. Furthermore, this was not in scope of the SAR to address.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

Seattle finds the proposed requirements are not backward compatible in that they significantly expand scope, from controls for access to BCSI about High and Medium-with-ERC BCS, to access to all High and Medium BCS. Although this change does address the conflict between the different BCSI applicabilities of CIP-004 and CIP-011, it does not seem necessary to address the objective of the SAR, which is to revise the Standards to clearly accommodate BCSI storage and use solutions that are not based on local, physically-focused concepts. Like the change proposed in Q1 above, it is a clarifying change but appears to do little or nothing to address the central object of these revisions.

If specific access controls are deemed desirable, Seattle recommends that the access termination requirement be changed from the unique-to-BCSI "one calendar day" to the "24 hours" that is used for all other access termination requirements.

Seattle also supports the comments of SMUD to this question.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	

Comment

We disagree with moving requirements for access to BCSI from CIP-004-6 to CIP-011-3 since it

causes unnessessay revisions of the exsiting CIP-004 and CIP-011 progroms without gaining any

security values. CIP-004 were originally developed for centralizing the access management within one standard and we don't think SDT wants backwards, otherwise, does electronic access and physical access need to be moved back to CIP-004 to CIP-007 and CIP-006 as well?	
Likes 0	
Dislikes 0	
Response	
Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy support the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

Disagree that the qualifying language “with ERC” was dropped from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 R4.1 when moved to CIP-011-3 R1.3. This deletion greatly expands the scope of this requirement. This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a considerable and sufficient protection in and of itself.

Lack of ERC also renders BCSI pertaining to Medium Impact BES Cyber Systems outside the scope of R1 Part 1.2, as any such information, if obtained, cannot be used remotely, as there is no remote access to the Cyber Systems. These Cyber Systems can only be compromised by breaching physical security, in which case this standard provides no protection.

There also is significant scope expansion with the authorization/revocation and review requirements now applying to all BCSI (not just designated storage locations of BCSI).

We disagree with moving requirements for access to BCSI from CIP-004-6 to CIP-011-3. We appreciate the attempt to streamline Requirements associated with BCSI by placing all related compliance activities solely within the CIP-011-3 Standard. However, by doing so Responsible Entities would be subject to the potential of having multiple compliance issues with one failed compliance activity as a result of the overlapping NERC CIP Standards.

For example, it is conceivable that one process could remove the ability to access BCSI as well as other logical access. In this approach if there was a failure in this process it could result in a violation of both CIP-004-7 R5 and for CIP-011-3 R1, where under current Standards this situation would result in a single potential non-compliance with CIP-004-6 R5.

Due to these reasons we suggest that access control Requirements remain in CIP-004-6 with other access control Requirements.

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 new standard expands the scope of BES CSI repositories to anywhere BES CSI may be, including in use and transit. This language is similar to the v3 language that was changed based on lessons learned. This may put entities across North America out of compliance because the current standard focuses on storage locations, not information in use or transit. Tracking BES CSI in use and transit will not be technically feasible and will but a great burden on business processes.

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller

Answer	No
Document Name	
Comment	
Due to having a strong disagreement with R1.2, 1.4 and R2, we disagree with this clarity statement.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	No
Document Name	
Comment	
While this change is minimal, it is relocated from the standard that contains all other authorization and provisioning requirements. This component of the requirement is about authorization, and is appropriate to be tracked and enforced in the same set of requirements, rather than potentially creating two separate violations when one violation would have occurred previously.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	No
Document Name	
Comment	
The requirment in CIP-011-3 R1.2 appears circular. Are we trying to elimiate the abiltiy to use the BCSI while we are using it? System Information by eliminating the ability to obtain and **use** BES Cyber System Information during, including storage, transit, **use**, and disposal .	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, 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 agrees the placement of access authorization and revocation as written in CIP-011-3, R1, Parts 1.3 and 1.5 does maintain backward compatibility to existing CIP-004 processes if an entity elects to use those existing processes. As noted in Question 1, PGAE does not agree storage locations need to be identified to establish the protections for the BCSI.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT agrees that the concepts of the current version of CIP-004 are maintained. However, a better approach may be to correct this with new parts in CIP-004. ERCOT also refers the drafting team to the comments submitted by ERCOT in response to Question No. 10.	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	

Answer	Yes
Document Name	
Comment	
We agree that the concepts of the current version of CIP-004 are maintained. However, a better approach would be to correct this with new parts in CIP-004. Also see comments on question 10.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG is in agreement with RSC provided comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NextEra	
Answer	Yes
Document Name	
Comment	
1. We agree this update is backward compatible and this update provides greater flexibility.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	

Comment	
We agree this update is backward compatible and this update provides greater flexibility.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees with moving the requirement to CIP-011. However, notes the change in applicabiltiy will be more than miminal effort to meet the new objectives.	
Likes 0	
Dislikes 0	
Response	
Calvin Wheatley - Wabash Valley Power Association - 1,3 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	

Likes 1	BC Hydro and Power Authority, 5, Hamilton Harding Helen
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
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	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
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	
Payam Farahbakhsh - Hydro One Networks, Inc. - 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	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
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	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
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	
William Hutchison - Southern Illinois Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	

Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	

3. The SDT is attempting to expand information storage solutions or security technologies for Responsible Entities. Do you agree that this approach is reflected in the proposed requirements?

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	No
Document Name	
Comment	
I cannot find these references in CIP-004-7. If you are referring to CIP-011-3, we see where you are trying to go, but we dont think that it is clear enough.	
Likes 0	
Dislikes 0	
Response	

Susan Sosbe - Wabash Valley Power Association - 3	
Answer	No
Document Name	
Comment	
The requirement mixes two types of usage needs. One is cloud storage and a separate requirement for vendors using information to perform work. The standard is appropriate for cloud storage type vendors. However, vendors using information for contract work should be moved or added to CIP-013 as part of an appropriate risk assessment.	
Likes 0	
Dislikes 0	
Response	

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	No
Document Name	
Comment	
There are too many ambiquities and additional clarity is required.	
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 increase in storage solutions adds ambiguity this could have been done in a more effective way by removing references to physical and electronic storage. If this new version is intended to allow Storage as a Service model by external vendors, it should be clearified. We recommend that the BES CSI also be clearified to define terms such as 'context'.

Likes 0	
Dislikes 0	

Response
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment
Cloud storage and encryption technologies are not excluded under the current standards. The ERO Enterprise CMEP Practice Guide: BES Cyber System Information dated April 26, 2019 suggests that CIP-004-6 and CIP-011-2 already accommodate BCSI on the cloud. We believe it would be better to focus efforts on Requirements that do not hinder the use of other solutions while allowing for the development of access control programs by Responsible Entities that address risk posed to the industry. Any new Requirements need to meet the objective of protecting access to BCSI without constraining or prescribing types of storage solutions.

Likes 0	
Dislikes 0	

Response
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy support the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
We disagree with the requirement language for achieving the SDT's goal. One of the SAR goals is to clarify the protections expected when utilizing third-party solutions (e.g., cloud services), but we haven't see the cloud storage and encryption language in the revised requirements yet.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
The revision succeeds in part but at the risk of considerable new ambiguities and unintended consequences (such as returning to the difficulty inherent in CIP v1-3 of controlling access to each individual piece of BCSI, or the necessity to understand the capability of an outside party to reasonably assess	

if they can “obtain and use” BCSI). The proposed language from CIP-011 R1.1 to R1.3 seems to Seattle a promising start to an objective-based, risk-focused approach to protection of BCSI, but then subsequent sub-requirements and requirements revert to an old-school prescriptive approach that creates confusion, speaks to specific technologies, and limits options. Seattle would prefer that a new Standard state a security objective, require a risk-based plan to meet this object (with certain, minimal components that must be in the plan), and then require implementation and periodic review of the plan.

Seattle also supports the comments of SMUD to this question.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Tri-State does not agree that this approach is aproppriately reflected in the proposed requirements. Some items allow for expanded use of BCSI solutions; however, the new R2 requirements are too prescriptive and cannot be prudently applied across all BCSI storage solutions and they limit the ability for the entity to manage their own compliance. Instead, these requirements should be objective based, which can be tailored to the specific solution and security options.

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 prescriptive and loses the focus on controlling access to BCSI. In its present form, it precludes technical advances that may improve how an RE controls access (e.g., geolocation, biometric, and other potential solutions).

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	
Comment	
Black Hills agrees that these changes make, what was understood to be possible under the current standards more explicit, however we are concerned that the standard remains too rigid. Instead we would prefer to see guidelines which then allow the RE to document its approach for using new technologies.	
Likes 0	
Dislikes 0	
Response	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	
Comment	
AECI supports comments filed by NRECA	
Likes 0	
Dislikes 0	
Response	

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	
Comment	
NRECA agrees that this is reflected in the proposed revisions; however, we are concerned that the way this has been incorporated places additional unnecessary compliance obligations on those entities that have chosen not to engage in the storage of BCSI in a cloud or other storage solution. Additionally, NRECA notes that the proposed revisions are very limiting relative to compatibility with future or differently configured storage solutions. For these reasons, NRECA is concerned that the proposed revisions will only work for specifically configured storage solutions and will not be properly scoped or flexible enough to accommodate the evolving storage and other solutions that could be employed in the future.	
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	
Agree with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
GSOC agrees that this is reflected in the proposed revisions; however, is concerned that the manner in which this has been incorporated places additional unnecessary compliance obligations on those entities that have chosen not to engage in the storage of BCSI in a cloud or other storage solution. Additionally, GSOC notes that the proposed revisions are very limiting relative to compatibility with future or differently configured storage solutions. Finally, GSOC respectfully asserts that standard revisions to accommodate cloud storage are unnecessary and would be better addressed in implementation or compliance guidance. For these reasons, GSOC is concerned that the proposed revisions will only work for specifically configured storage solutions and will not be properly scoped or flexible to enough to accommodate the evolving storage and other solutions that could be employed in the future.	
Likes 0	
Dislikes 0	
Response	

Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC agrees with comments submitted by NRECA.	
Likes 0	
Dislikes 0	
Response	

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Yes, agree that a stand alone requirement where a vendor stores an entitiy's BCSI is needed. 1.4.1 requires an initial risk assessment of vendors but the SDT needs to define what is acceptable evidence for a risk assessment.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
It is unclear in this draft or guidance how the SDT is expanding information storage soluctions or security technologies.	
Likes 0	
Dislikes 0	
Response	
Vivian Moser - APS - Arizona Public Service Co. - 3	
Answer	No
Document Name	
Comment	
Although AZPS agrees that the SDT's intent is reflected in Part 1.4, the requirements as written do not clearly reflect an approach to expand information storage solutions or security technologies.	
Likes 0	
Dislikes 0	
Response	

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
New and emerging technologies shift the paradigm of security controls away from a specific storage location/repository to the ability to access and use the information itself. For example, an entity that utilizes file level security can apply encrypted protections on the data that preclude unauthorized access to the data regardless of where it is stored. Requiring a list of storage locations is an antiquated construct that disincentivizes entities from using potentially more secure mechanisms because of the impossibility of compliance with documenting storage locations. The requirement should be technology agnostic and objective based, so it is written to focus on the implementation of effective methods that afford adequate security protections to prevent unauthorized access to the information	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3	
Answer	No
Document Name	
Comment	
Tri-State G&T does not agree that this approach is apropppriately reflected in the proposed requirements. Some items allow for expanded use of BCSI solutions however, the new R2 requirements are too prescriptive and cannot be prudently applied across all BCSI storage solutions and they limit the ability for the entity to manage their own compliance. Instead, these requirements should be objective based, which can be tailored to the specific solution and security options.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
See NRECA submitted comments.	

Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
While N&ST understands one of the SDT's key goals is to facilitate the use of an expanded array of storage options, we believe the associated imposition of a specific technology (encryption + key management) is likely to inhibit, not promote, the use of newer storage options such as cloud-based solutions. Furthermore, N&ST is concerned that the SDT's proposed changes could have significant cost and effort impacts on Responsible Entities that neither store BCSI in the cloud today nor have any plans to do so in the future.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We disagree because cloud based storage technologies and encryption technologies are not excluded under the current standards. The ERO Enterprise CMEP Practice Guide stated: BES Cyber System Information dated April 26, 2019 suggests that CIP-004-6 and CIP-011-2 already accommodates BCSI on the cloud.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	

Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren agrees with and supports EEI comments.

Likes 0	
Dislikes 0	

Response

Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC

Answer	No
Document Name	

Comment

NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES

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

The question asks if the approach expands two different things: information storage solutions and security technologies. We agree the changes could allow for expanded storage solutions, but we do not agree that this approach expands security technologies for Responsible Entities. An example of a

security technology may be a cloud service that needs to use the information in order to provide security or reliability benefit to the BES. We find an applicable phrase in the “Industry Need” section of the SAR that states the expected reliability benefit is “providing a secure path towards utilization of modern third-party data storage **and analysis** systems” and the current draft doesn’t address third party analysis of the data to provide services to entities and actually further restricts such analysis.

It seems the approach is focused solely on using cloud storage for BCSI in an encrypted form and managing the encryption keys. Therefore, the focus seems to be on cloud **storage** only, not cloud **services** that need to use or analyze the data to provide services such as security monitoring technologies.

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

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 response found in the NSRF Comment Form

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	
Comment	

We disagree with the proposed approach, as we do not see the necessity. Cloud-based storage technologies and encryption technologies are not excluded either under the current standards, or by the ERO Enterprise CMEP Practice Guide BES Cyber System Information dated April 26, 2019.

We agree with EEI comments that requirements should neither constrain nor prescribe solutions.

Likes 0	
Dislikes 0	
Response	

Ayman Samaan - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	
Comment	

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	
Response	

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	No
Document Name	
Comment	

We appreciate the SDT's effort to expand information storage solutions and security technologies; however, key management is the only technology that is explicitly detailed within the requirements. We feel that this is contradictory to what the 2016-02 SDT is working to accomplish with risk-based standards. Additionally, as the requirement is currently written, an entity would need to prove a negative if this requirement is not applicable to them, which is administratively burdensome. Finally, while it might not have been the SDT's intent, an auditor might interpret the requirement to mean that if an entity uses encryption internally (not with a third-party), then that entity must have a key management program, based on the requirement, for their internal encryption.

Likes 0	

Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support MRO comments.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
The standards development team should support specific requirements providing appropriate levels of security for Cloud Service Providers and 3rd Party Access. Transferring the CIP-004 BCSI requirements to CIP-011 does not address the unique issues created by storing BCSI in repositories that are not controlled by registered entities. The standards development team should draft separate requirements.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
MISO’s response assumes this question pertains to all proposed changes in CIP-011, requirement R1 (parts 1.1 – 1.5). The proposed changes as written, do not clearly draw out / articulate key distinctions that were noted during the Q&A portion of the 2019-02: BES Cyber System Information Access Management Webinar hosted on January 16, 2020: physical or electronic, responsible entity or vendor hosted. To make this clear in the proposed standard, MISO proposes the SDT include the following changes.	

Part 1.1. Modify the last example provided under Measures to read as follows: “Storage locations *(physical or electronic, responsible entity or vendor hosted)* identified for housing BES Cyber System Information in the entity’s information protection program.”

Part 1.2 For clarity, modify the bullet under Measures as follows: “Evidence of methods used to prevent the unauthorized access to BES Cyber System Information (e.g., encryption of BES Cyber System Information, [delete the word "and"] key management program, retention in the Physical Security Perimeter).”

Part 1.3 May not be necessary if the SDT accepts MISO’s proposal to retain all access management provisions (BCS and BCSI) as part of CIP-004-7.

Part 1.4 MISO recommends the provisions in this section be eliminated from CIP-011-3 and addressed as part of CIP-013-2 thereby covering all vendor requirements (BCS and BCSI) in the same standard.

Part 1.5 MISO recommends the provisions in this section be eliminated from CIP-011-3 and addressed as part of CIP-004-7, requirement R5.3 thereby covering all access management requirements (BCS and BCSI) in the same standard.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

No, this approach is not clearly reflected in the proposed requirements. If the SDT’s intent is to provide direction on protection of BCSI stored in the cloud, it should be clearly stated by saying that these requirements are intended to address vendor operated storage locations or services. The vague language of “in cases where vendors store Responsible Entity’s BES Cyber System Information” opens a broad potential for auditor interpretation with unintended applicability, including instances where data has been shared with a vendor, but the vendor is not operating a storage location, or where a corporate resource with cloud functions is used to store working copies of data but is not a designated storage location.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

EEI appreciates the SDT efforts to expand information storage solutions or security technologies for responsible entities. However, the proposed approach appears to be too prescriptive and inconsistent with elements of a results-based standard. The SDT should also ensure that the requirements are not tailored to any one solution or technology.

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2

Answer	No
Document Name	

Comment

NYISO's response is based on the assumption this question pertains to all proposed changes in CIP-011, requirement R1 (all subsections).

NYISO feels that the proposed changes do not clearly draw out or articulate key distinctions that were presented within the Q&A portion of the 2019-02: BES Cyber System Information Access Management Webinar hosted on January 16, 2020. NYISO feels that additional language be inserted to account for use cases (physical or electronic data being housed within either the responsible entity's controlled data centers or instances where the responsible entity has chosen to use vendor-hosted storage.

To make this clearer, NYISO proposes the SDT include the following changes:

Within Part 1.1: Modifications be made to the last example provided under Measures to read:

"Storage locations (physical or electronic, responsible entity or vendor hosted) be identified as housing BES Cyber System Information in the entity's information protection program."

Within Part 1.2: For clarity, modify the bullet under Measures to read:

"Evidence of methods used to prevent the unauthorized access to BES Cyber System Information (e.g., encryption of BES Cyber System Information with a sound key management program, retention within the responsible entity's Physical Security Perimeter)."

NYISO feels that Part 1.3 will become unnecessary if the SDT retains all access management provisions (BCS and BCSI) within CIP-004-7.

NYISO would recommend that provisions contained in the current draft within Part 1.4 be removed from CIP-011-3 and addressed as part of CIP-013-2. This would have the effect of keeping all vendor requirements (BCS and BCSI) within the same standard.

NYISO would recommend that the provisions contained in the current draft within Part 1.5 be removed from CIP-011-3 and addressed as part of CIP-004-7. This would have the effect of keeping all access management requirements (BCS and BCSI) within the same standard.

Overall, NYISO would like to see all of the requirements in R1 be made clearer to allow the Responsible Entity latitude to choose any applicable security technologies that adequately protects BCSI, based on risk. Within the current draft, the language within R2 suggests that key management programs are mandatory; however, NYISO believes the intent was to allow other methods of protections as supported options.

Likes 0	
Dislikes 0	

Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
We believe the existing standard already allows multiple solutions. Why won't NERC/FERC tell Entities that the standard does not limited the scope of solutions available to entities and be done with this?	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
No, SNPD does not believe the SDT's objective has been met. SNPD believes that without explicit, affirmative authorization to use managed service ("cloud") storage solutions, Entities cannot and likely will not feel confident storing BCSI in the cloud. Entities will likely take the most conservative response to avoid potential compliance risk and simply choose not to use cloud storage solutions. Thereby, maintaining the status quo and depriving Entities of the flexibility desired under the proposed change. Suggestion: establish "reciprocity" from current Federal IT certification standards such as FedRAMP/FISMA/DoD D-ITAR. Issue a blanket statement that storage of BCSI is authorized in any/all FedRAMP/FISMA or DoD D-ITAR cloud. This type of verbiage is both actionable and clear.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	

While Alliant Energy appreciates the SDT's efforts to expand information storage solutions or security technologies for responsible entities, that expansion is only useful if the requirement language is written such that it is clearly auditable. The updated requirements should avoid the ability to audit to prescriptive requirements that are not stated in the language of the requirements.

Likes 0	
Dislikes 0	

Response

Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3

Answer	No
Document Name	

Comment

See Steven Toosevich's comments.

Likes 0	
Dislikes 0	

Response

James Brown - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

There is no expansion of solutions or technologies used. The proposed requirements codify the controls that have been discussed in informal manners. This is a slight improvement, but as long as CIP requirements can also be interpreted as applicable for cloud vendors and are in the audit scope of CIP audits, there is no real improvement.

Recommend excluding cloud vendors from applicability column of BCSI requirements and, instead setting requirements to be included in risk assessments of cloud vendors and have the CIP senior manager or delegate approve each assessment and applicable risk mitigations at minimum intervals. In addition cloud vendor requirements appears to be better addressed through CIP-013.

BCSI related cloud vendor risk assessment components can be a subset of CIP004 or CIP011 requirements that meet cloud vendor industry best practices such as the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ) and the provision of certifications (e.g. ISO 27000) or audit reports (e.g. SOC for security) from accredited auditors who have verified cloud vendor claims of compliance.

Likes 0	

Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE agrees with EEI's comments	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	No
Document Name	
Comment	
No, in order to provide expanded security technology solutions (read "in the cloud"), the vendor may need both access and use of BCSI to provide any value to the registered entity. The approach offered in this proposal does not allow this access.	
Likes 0	
Dislikes 0	
Response	
Angela Gaines - Portland General Electric Co. - 1	
Answer	No
Document Name	
Comment	
Please see comments PGE Group 2	
Likes 0	

Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
We believe the existing standard already allows multiple solutions. Why won't NERC/FERC tell Entities that the standard does not limited the scope of solutions available to entities and be done with this?	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
We disagree with the proposed approach, as we do not see the necessity. Cloud-based storage technologies and encryption technologies are not excluded either under the current standards, or by the ERO Enterprise CMEP Practice Guide BES Cyber System Information dated April 26, 2019. We agree with EEI and MRO NSRF comments that requirements should neither constrain nor prescribe solutions.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
There is no expansion of solutions or technologies used. The proposed requirements codify the controls that have been discussed in informal manners. This is a slight improvement, but as long as CIP requirements can also be interpreted as applicable to cloud vendors, and are in the scope of CIP audits, there is no real improvement.	

ERCOT recommends excluding cloud vendors from the applicability column of BCSI requirements, and instead setting requirements to be included in risk assessments of cloud vendors and having CIP senior managers or delegates approve each assessment and applicable risk mitigations at minimum intervals. In addition, cloud vendor requirements appear to be better addressed through CIP-013.

BCSI related cloud vendor risk assessment components can be a subset of CIP-004 or CIP-011 requirements that meet cloud vendor industry best practices such as the Cloud Security Alliance (CSA), Consensus Assessments Initiative Questionnaire (CAIQ), and the provision of certifications (e.g. ISO 27000) or audit reports (e.g. SOC for security) from accredited auditors who have verified cloud vendor claims of compliance.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

We disagree with the proposed approach, as we do not see the necessity. Cloud-based storage technologies and encryption technologies are not excluded either under the current standards, or by the ERO Enterprise CMEP Practice Guide BES Cyber System Information dated April 26, 2019.

We agree with EEI and MRO NSRF comments that requirements should neither constrain nor prescribe solutions.

Likes 0	
Dislikes 0	
Response	
Colleen Campbell - AES - Indianapolis Power and Light Co. - 3	
Answer	No
Document Name	
Comment	
There has to be a better definition of the different storage and security technologies the SDT is considering. There will be a big difference between on premise and external solutions.	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
Comments: While there is clearly an effort to address expanded use of information storage solutions and security technologies, the current draft does not specifically address use cases associated with cloud services and information sharing with external parties as clearly as will be required. For entities to make use of options available from external service providers, there will need to be specification of information protections specific to such situations (i.e. whether individual access to information must be demonstrated by the service provider to the responsible entity and the expectations for measures to demonstrate compliance of a third party).	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	

SunPower agrees with MRO NSRF's comments	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
Likes 1	BC Hydro and Power Authority, 5, Hamilton Harding Helen
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

William Hutchison - Southern Illinois Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Comments: Although the language allows Entities to expand information storage solutions, it then leaves the Entity open to risk due to interpretation of how their process and security measures are interpreted by an auditor. As long as there is consistency in audit, that if an Entity follows their process, as required by the standard, no audit findings will be given. If an auditor takes issue with the Entity's process(es) or security technology, an audit recommendation would be given, not a finding and or associated fine.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees that this approach is reflected in the proposed requirements. However, the requirements as written are problematic for reasons provided in subsequent responses.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3	
Answer	Yes
Document Name	
Comment	
AEP is of the opinion that the approach to expand information storage solutions is reflected in the proposed modifications. However, we feel that while this approach may help organizations having information storage isssues, we also feel that this approach produces security concerns as a result of BCSI being stored using cloud technology.	
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	
Although the language allows Entities to expand information storage solutions, it then leaves the Entity open to risk due to interpretation of how their process and security measures are interpreted by an auditor. As long as there is consistency in audit, that if an Entity follows their process, as required by the standard, no audit findings will be given. If an auditor takes issue with the Entity's process(es) or security technology, an audit recommendation would be given, not a finding and or associated fine.	
Likes 0	
Dislikes 0	

Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	

Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	
Yes the expanded approach is available in the proposed standard; however, as discussed later, the requirements need to be improved.	
Likes 0	
Dislikes 0	

Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, 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	
PGAE believes the modifications expand the capability to use third-party service providers without a risk of being non-compliant based on different interpretations of the current Standards. The method(s) or technology used to protect the BCSI are non-prescriptive, providing the necessary flexibility to meet the objective of preventing unauthorized access.	
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	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
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	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
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	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
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	
Likes 0	
Dislikes 0	
Response	

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NextEra	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	

4. The SDT is addressing, and further defining, the risk regarding potential compromise of BCSI through the inclusion of the terms “obtain” and “use” in requirement CIP-011-3, Requirement R1 Part 1.2. Do you agree that this will more accurately address the risk related to the potential compromise of BCSI versus the previous approach?

Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	

1.2 becomes extremely burdensome by eliminating the ability to obtain and use BCSI during storage, transit, use, and disposal. Entities may need to employ methods such as chain of custody for disposal of hard drives that may contain BCSI.

SunPower encourages the term “reduce” the ability to obtain and use BES Cyber System Information during storage, transit, use. . .

Likes 0	
Dislikes 0	
Response	

Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	

Comments:

The inclusion of the terms “obtain and use” help to more accurately identify the objective of the access protections that need to be implemented. However, inclusion of those terms does not accurately address the risk related to the potential compromise of BCSI.

Moreover, the term “eliminating” is an absolute, so implementation and compliance would be challenging to demonstrate.

Recommendation: change the language to “methods to prevent the ability to obtain and use BCSI information through unauthorized access including storage, transit, use and disposal.”

Likes 0	
Dislikes 0	
Response	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	

Comment
The previous Part 1.2 approach gave Responsible Entities flexibility to accurately address the risk related to the potential compromise of BCSI. The new Part 1.2 approach does not appear to give Responsible Entities thae same flexibility, especially if third-party solutions (e.g., cloud services) are not utilized. If the purpose of the new Part 1.2 approach is to address the risk associated with the use of a third-party solution (e.g. cloud services), the Part 1.2 requirement language should be made more clear than is currently proposed. IPC requests that the SDT provide additional rationale information related to “the ability to obtain and use BES Cyber System Information” language in the proposed requirement as it is unclear what is intended by the phrase “obtain and use” in the requirement. IPC believes the Part 1.2 requirement language should focus more on a Responsible Entity ensuring they have appropriate measures in place within their BES Cyber System Information (BCSI) Protection Program to protect BCSI rather than requiring entities to encrypt their data in transit, storage, and use.

Likes 0	
Dislikes 0	

Response

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

Comment
Agree with terms “obtain” and “use;” however, more explanation is needed within the requirement or guidelines. The drafting team has referred to the CMEP BCSI practice guide. We recommend defining “BCSI Access” in the NERC Glossary of Terms per the practice guide: “An instance or event during which a user obtains and uses BCSI. For access to occur, in this context, a user, authorized or unauthorized, must concurrently both obtain BCSI and possess the ability to use BCSI. An unauthorized individual who obtains encrypted BCSI but has no ability to use it within a meaningful timeframe should not be considered to have access.” The draft R1 Part 1.2 Requirement could then be revised to “Method(s) to prevent unauthorized BCSI Access during BCSI storage, transit, and use.” We disagree with the phrase, “by eliminating the ability” to obtain and use. This represents an unachievable threshold over and above the current “Procedure(s) for protecting and securely handling.” We concur with MRO NSRF comments that disagree with the addition of “and disposal” to the end of the requirement. BCSI in BES Cyber Systems is already addressed in R3 Part 3.1., but Part 3.1 needs to reinstate the qualifying language in the Requirements “that contain BES Cyber System Information.” Deletion of this qualifying language is an expansion of scope to the current CIP-011-2 R2 requiring evidence of sanitization of assets not containing BCSI subject to this protection. Although a logical inclusion as part of the lifecycle of BCSI, as applied in R1 Part 1.2, the Measures would need to address examples of acceptable evidence of disposal, such as shredding for paper. We do not see a practical method of evidencing the disposal of electronic BCSI, i.e. the day-to-day deletion of electronic files.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Agree with terms “obtain” and “use;” however, more explanation is needed within the requirement or guidelines. The drafting team has referred to the CMEP BCSI practice guide. We recommend defining “BCSI Access” in the NERC Glossary of Terms per the practice guide: “An instance or event during which a user obtains and uses BCSI. For access to occur, in this context, a user, authorized or unauthorized, must concurrently both obtain BCSI and possess the ability to use BCSI. An unauthorized individual who obtains encrypted BCSI but has no ability to use it within a meaningful timeframe should not be considered to have access.”

The draft R1 Part 1.2 Requirement could then be revised to “Method(s) to prevent unauthorized BCSI Access during BCSI storage, transit, and use.”

We disagree with the phrase, “by eliminating the ability” to obtain and use. This represents an unachievable threshold over and above the current “Procedure(s) for protecting and securely handling.”

We concur with MRO NSRF comments that disagree with the addition of “and disposal” to the end of the requirement. BCSI in BES Cyber Systems is already addressed in R3 Part 3.1., but Part 3.1 needs to reinstate the qualifying language in the Requirements “that contain BES Cyber System Information.” Deletion of this qualifying language is an expansion of scope to the current CIP-011-2 R2 requiring evidence of sanitization of assets not containing BCSI subject to this protection.

Although a logical inclusion as part of the lifecycle of BCSI, as applied in R1 Part 1.2, the Measures would need to address examples of acceptable evidence of disposal, such as shredding for paper. We do not see a practical method of evidencing the disposal of electronic BCSI, i.e. the day-to-day deletion of electronic files.

Likes 0	
Dislikes 0	

Response

Angela Gaines - Portland General Electric Co. - 1

Answer	No
Document Name	

Comment

Please see comments PGE Group 2

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

There appears to be a significant challenge with the proposed wording of Requirement Part 1.2, which appears to require entities to eliminate the ability to obtain and use BCSI even for authorized access holders.

Suggest the following replacement requirement text:

"Method(s) to prevent unauthorized access to BES Cyber System Information by eliminating the ability of unauthorized users to obtain and use BES Cyber System Information during storage, transit, use, and disposal."

OR

"Method(s) to prevent unauthorized access to BES Cyber System Information by restricting the ability to obtain and use BES Cyber System Information during storage, transit, use, and disposal, to authorized access holders."

While this approach is better than previous approaches, there is still a need for security technology vendor service providers to have access and use of BCSI. The proposed update does nothing to allow MSSPs in a CIP program. Along with allowing Authorized users to both obtain and use, the EACMS split to EACS and EAMS is also required to allow MSSPs.

Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE agrees with EEI’s comments	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	No
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI’s comments.	
Likes 0	
Dislikes 0	

Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
SNPD does not agree that this will more accurately address the risk related to the potential compromise of BCSI versus the previous approach and verbiage. However, SNPD supports the reasoning behind the proposed change.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro requests more clarity as to what is the extent of the application of the term “elimination” that is now included in the requirement. Please add clarity within the language of standard. Example: Is an encryption key sufficient to “eliminate” even though this is potentially hackable? BC Hydro would also request additional clarity on what the “ability to use BCSI” means.	
Likes 1	BC Hydro and Power Authority, 5, Hamilton Harding Helen
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI has concerns with defining risks regarding potential compromise of BCSI within the language of a Reliability Standard. EEI suggests that it may be simpler to address BCSI security concerns through the development of a definition for “Useable Access” within the NERC Glossary of Terms. We also suggest the SDT consider using the language from the April 26, 2019, ERO Enterprise CMEP Practice Guide on BES Cyber System Information which	

appears to have the requisite clarity and could act as a clear definition for “Useable Access” (see below). If the term is deemed to be unsuitable, the SDT could use the phrase “Access to the BCSI….”

Useable Access: An instance or event during which a user obtains and uses BCSI. For access to occur, in this context, a user, authorized or unauthorized, must concurrently both obtain BCSI and possess the ability to use BCSI. An unauthorized individual who obtains encrypted BCSI but has no ability to use it within a meaningful timeframe should not be considered to have access. Ref.: Page 2, Bullet 1: https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/ERO%20Enterprise%20CMEP%20Practice%20Guide%20_%20BCSI%20-%20v0.2%20CLEAN.pdf

In consideration of access, CIP-004-6 already effectively addresses access controls for BCSI when stored by responsible entities at their facilities so protections would only need to be developed for a situation where third party cloud-based services are used. Consequently, the above reference *CMEP Practice Guide* could effectively define access in a manner that addresses this issue.

Within this alternative approach and once the definition for “Useable Access” is addressed, the changes needed to meet the intent of the SAR could be simply accomplished through the following changes to CIP-004-6:

4.1.1. Electronic Access

4.1.2. Unescorted physical access into a Physical Security Perimeter; and

4.1.3. Useable Access to a BCSI Repository

The SDT should also consider restoring the language of CIP-004-6 R5.3, with the modification as shown below, or something similar, that achieves a similar result:

*For termination actions, revoke the individual’s **Useable Access** to **a BCSI Repository**, 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.*

With the proposed solution, the language within CIP-004-6, Part 5.3 could be largely retained while limiting the scope of any vendor’s “Useable Access.” In such a situation, the vendor is simply a custodian to encrypted or otherwise masked data and does not have the ability to use it. Additionally, vendors with “Useable Access” (i.e., both custody of data and ability to use BCSI) would continue to need provisional access granted by the responsible entity through their established access control process and procedures.

Lastly, EEI is concerned with the compliance issues in using the term “eliminate” as proposed in CIP-011-3 R1.2. The word “eliminate” is ambiguous when considered within the context of demonstrating compliance. It will be difficult to prove to an auditor that the responsible entity has eliminated all risk. EEI suggests that the SDT modify the language and replace “eliminate” with “limit” or some similar language.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

CEHE recommends using the words “or” instead of “and” and proposes the following alternative:

"Method(s) to prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain or use BES Cyber System Information during storage, transit, use, and disposal."

Protections to prevent access, like access control to the storage location, are separate and distinct from controls to prevent use, like encryption during transit. Entities may have systems with one but not the other, if the system is all in house and physically protected. The proposed language would not be backward compatible.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The standards development team should support specific requirements providing appropriate levels of security for Cloud Service Providers and 3rd Party Access. Transferring the CIP-004 BCSI requirements to CIP-011 does not address the unique issues created by storing BCSI in repositories that are not controlled by registered entities. The standards development team should draft separate requirements.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support MRO comments.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment
While we agree that “obtain” and “use” more accurately address the risk, we have concerns with the overall wording. One of the below listed changes should be made to these modified Standards. We recommend changing Part 1.2 from <<Method(s) to prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BES Cyber System Information during, including storage, transit, use, and disposal.>> To <<Method(s) to prevent the ability to obtain and use BES Cyber System Information through unauthorized access during, including storage, transit, use, and disposal.>> because “eliminating” is an absolute which makes implementation and demonstrating Compliance too challenging.

Likes 0	
Dislikes 0	

Response

Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	

Comment
Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	

Comment
Agree with terms “obtain” and “use;” however, more explanation is needed within the requirement or guidelines. The drafting team has referred to the CMEP BCSI practice guide. We recommend defining “BCSI Access” in the NERC Glossary of Terms per the practice guide: “An instance or event during which a user obtains and uses BCSI. For access to occur, in this context, a user, authorized or unauthorized, must concurrently both obtain BCSI

and possess the ability to use BCSI. An unauthorized individual who obtains encrypted BCSI but has no ability to use it within a meaningful timeframe should not be considered to have access."

The draft R1 Part 1.2 Requirement could then be revised to "Method(s) to prevent unauthorized BCSI Access during BCSI storage, transit, and use."

We disagree with the phrase, "by eliminating the ability" to obtain and use. This represents an unachievable threshold over and above the current "Procedure(s) for protecting and securely handling."

We concur with MRO NSRF comments that disagree with the addition of "and disposal" to the end of the requirement. BCSI in BES Cyber Systems is already addressed in R3 Part 3.1., but Part 3.1 needs to reinstate the qualifying language in the Requirements "that contain BES Cyber System Information." Deletion of this qualifying language is an expansion of scope to the current CIP-011-2 R2 requiring evidence of sanitization of assets not containing BCSI subject to this protection.

Although a logical inclusion as part of the lifecycle of BCSI, as applied in R1 Part 1.2, the Measures would need to address examples of acceptable evidence of disposal, such as shredding for paper. We do not see a practical method of evidencing the disposal of electronic BCSI, i.e. the day-to-day deletion of electronic files.

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 response found in the NSRF Comment Form

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	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
The language of "eliminating the ability to obtain the and use BES Cyber Information" sounds ambiguous. Also, the term "use" that occurs twice within a sentence need more clarification.	
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	

We do not agree with the modifications to Part 1.2 for the following reasons:

- It requires methods to "prevent" unauthorized access. We caution against using "100% words" in situations such as this because if ever a piece of encrypted information is cracked, the entity's method did not 100% prevent it. A technology breakthrough or suddenly discovered vulnerability in an encryption algorithm that enables cracking today's encryption protocols makes the entire industry suddenly non-compliant.

- R1.2 goes on to say the process must prevent unauthorized access BY eliminating the ability to obtain and use BCSI. A literal reading of this requirement says that entities must prevent unauthorized access by eliminating ALL ability for anyone to obtain and use BCSI. We understand this phrasing is attempting to define "access", but the way this is stated it says you must prevent unauthorized access by eliminating all access.

- Adding “disposal” to R1.2 is duplicative of R3. That’s now required twice in two different requirements within the same standard, and we do not support including it here. We also question how “disposal” of BCSI is not inherently included in “storage, transit, and use” and why the additional qualifier is needed?

Likes 0	
Dislikes 0	

Response

Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC

Answer	No
Document Name	

Comment

NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren agrees with and supports EEI comments.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

BPA understands “obtain” to mean take possession of, and “use” to mean take an action on. “Obtain” is not much clearer than “gain access to” while “use” does add an element of clarity to the objective of what needs to be protected. “Use” implies that obtaining “unusable” (i.e., encrypted) information is a lesser risk.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We agree with using the terms “obtain” and “use”. However, this will require the Responsible Entity document what the the terms “obtain” and “use” mean with respect to BCSI – we believe more explanation is needed within the requirement or guidelines.

Based on the CMEP BCSI practice guide. The practice guide provides very little additional information on what is meant by “obtain” and “use.” Without additional guidance evidencing this concept for audit purposes (that someone obtained BCSI but couldn’t use it) would be a significant challenge.

We disagree with the phrase, “by eliminating the ability” to obtain and use. This represents an unachievable threshold over and above the current “Procedure(s) for protecting and securely handling.”

Likes 0	
Dislikes 0	

Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST does not believe the proposed terms will enhance general understanding of the risks associated with potential compromises of BCSI. In N&ST's opinion, the NERC Glossary definition of BCSI ("Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System.") more than adequately defines the potential risks. Furthermore, in recent discussions with representatives from several Responsible Entities, it has become apparent to N&ST that there is NO good consensus on what it means to "use" BCSI. We believe the existing language in CIP-011-2, Requirement R1 Part 1.2 should be retained.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
See NRECA submitted comments. For key retention in R1.2 of CIP-011, is this saying that where the key is stored needs to be behind a PSP?	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3	
Answer	No
Document Name	
Comment	
Tri-State G&T does not agree. Clarity is needed around what "use" means, especially considering this is an issue that currently exists under the version that is in effect. Similarly, there would need to be more clarity around the meaning of the term "obtain".	

As for R1.2, we think the original language (other than “use” not being defined) was correct and the concept of “obtain and use” should instead be incorporated into the access requirements, especially R1.3. This will make it clear that in order for someone to be deemed to have access to BCSI, they must have the ability to obtain and use it, which would align with the ERO Practice Guide. Although, we don’t recommend using the actual terms “use” and “obtain”, without providing more clarification as to their meaning.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

The intention is good; however, the current proposed requirement language does not accomplish that intention; instead it seems to completely preclude the use of BCSI the way it is written.

Likes 0	
Dislikes 0	

Response

Vivian Moser - APS - Arizona Public Service Co. - 3

Answer	No
Document Name	

Comment

While AZPS agrees that the inclusion of “obtain” and “use” more clearly addresses the risk related to the potential compromise of BCSI, AZPS believes that the proposed language in Part 1.2 creates an undue burden for Entities to execute and evidence “eliminating the ability to obtain and use BES Cyber System Information during storage, transit, use, and disposal”. AZPS recommends that the SDT retain focus of the requirement language on “protecting and securely handling” BCSI, and address the inclusion of “obtain” and “use” in guidance documents. AZPS offers proposed changes for Part 1.2 below:

“Procedure or method(s) to prevent unauthorized access, protect, and securely hande BES Cyber System Information during storage, transit, use, and disposal”.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
WAPA requests changing the work “use” in the last sentence of the requirement. “BES Cyber System Information during storage, transit, use and disposal.” To “BES Cyber System Information during storage, transit, and disposal. The lack of a clear definintion for the word “use” creates major problems for Registered Entities (REs). Use in context of BCSI displayed a system screen, BCSI layed out on a drafting table, BCSI posted in a response/job aid binder being read by an aoperator or BCSI in computer systems memory address? Without a better definition REs will need to implement procedures to address these scenarios; some of which are not commercially viable (memory encryption).	
Likes 0	
Dislikes 0	
Response	

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
The change made to CIP-011-3 Part 1.2 does not add clarity. The choice of the second “use” in Part 1.2 is confusing and does not make sense; “…by eliminating the ability to obtain and use BES Cyber System Information during, storage, transit, use, and disposal.” The standards drafting team needs to elaborate on “…eliminating the ability…” The SDT should remove the second “use”.	
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	
It is impossible to completely “prevent” and or “eliminate” the ability to obtain and or use BCSI during storage, transit, use, and disposal, so all Entities would be in violation the way this is written. The reasons the standards exist are to lower cyber security risks to the BPS. Suggest replacing “eliminating” with “reducing” or rewording the requirement language to: “Method(s) to reduce the risk of unauthorized access to BCSI during storage, transit, use and disposal.”	

Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC agrees with comments submitted by NRECA.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
GSOC agrees that the approach essentially “eliminates” the risk associated with use of BCSI as the revisions require entities to completely eliminate the ability to obtain or use BCSI during nearly all life stages with the exception of creation. GSOC respectfully suggests that use of the term “eliminate” was inadvertent and should be revised to “control” or “restrict.” Should the SDT remove the term “eliminate” and replace it with a feasible alternative, this requirement could achieve its intended purpose. However, GSOC also notes, for the SDT’s consideration, the infeasibility of the term “prevent.” Responsible Entities cannot “prevent” or “eliminate” every risk or capability that could possibly manifest during the life cycle of BCSI. Further, it is difficult to conceive of how prevention of “unauthorized access” would be documented and proven during compliance monitoring. For this reason, GSOC recommends that the SDT revise the requirement to indicate an affirmative obligation to manage or control access rather than an obligation to prevent access, which would effectively require Responsible Entities to “prove” that unauthorized access did not occur rather than proving that they “controlled” or “managed” access through proactive security controls. Such a revision will not only reduce the potential for confusion around whether unauthorized access was “prevented,” it will also remove the likelihood that Responsible Entities would be required to “prove a negative” during compliance monitoring activities. For these reasons, GSOC recommends that the SDT consider revising the requirement as proposed below. Method(s) to manage access to BES Cyber System Information during storage, transit, use, and disposal.	
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	

While we appreciate the SDT's effort to clarify what access means, this is better left to guidance documents, like it is now in the CMEP Practice Guide: BES Cyber System Information, dated April 26, 2019. Without the additional context that the guidance document provides, this language just adds confusion to the requirement. In addition, the ability to *use* information is open to interpretation, such as whether or not the individual has the knowledge to use the information in such a way as to affect the BES.

Also, it is not possible to completely *eliminate* the ability to obtain and use BCSI, so "eliminate" should not be used.

Likes 0	
Dislikes 0	
Response	

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	

NRECA agrees that the approach essentially "eliminates" the risk associated with use of BCSI as the revisions require entities to completely eliminate the ability to obtain or use BCSI during nearly all life stages with the exception of creation. NRECA believes that use of the term "eliminate" was inadvertent and should be revised to "control" or "restrict." Should the SDT remove the term "eliminate" and replace it with a feasible alternative, this requirement could achieve its intended purpose. However, NRECA also notes, for the SDT's consideration, the infeasibility of the term "prevent." Responsible Entities cannot "prevent" or "eliminate" every risk or capability that could possibly manifest during the life cycle of BCSI. Further, it is difficult to conceive of how prevention of "unauthorized access" would be documented and proven during compliance monitoring.

For this reason, NRECA recommends that the SDT revise the requirement to indicate an affirmative obligation to manage or control access rather than an obligation to prevent access, which would effectively require Responsible Entities to "prove" that unauthorized access did not occur rather than proving that they "controlled" or "managed" access through proactive security controls. Such a revision will not only reduce the potential for confusion around whether unauthorized access was "prevented," it will also remove the likelihood that Responsible Entities would be required to "prove a negative" during compliance monitoring activities. For these reasons, NRECA recommends that the SDT consider revising the requirement as proposed below:

"Method(s) to "manage" access to BES Cyber System Information during storage, transit, use, and disposal."

Likes 0	
Dislikes 0	
Response	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI supports comments filed by NRECA	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3	
Answer	No
Document Name	
Comment	
AEP does not believe that the new language being proposed effectively addresses risks associated the compromise of BCSI. AEP has no opinion on the inclusion of the words “obtain” and “use”, but the inclusion of the word “eliminating” is a cause for concern. The absolute nature of the word has brought about concerns that it would be difficult to prove compliance.	
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 removal of the word “designated” creates an insurmountable scope of program management. The use of the word “eliminate” sets an impossible threshold to achieve.	
Likes 0	
Dislikes 0	
Response	

Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
There are issues with the wording. "eliminating the ability to obtain and use BES Cyber System Information during, including storage, transit, use, and disposal"	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State does not agree. Need more clarity around what "use" means, especially considering this is an issue that currently exists under the version that is in effect. Similarly, there would need to be more clarity around the meaning of the term "obtain". As for R1.2, we think the original language (other than "use" not being defined) was correct and the concept of "obtain and use" should instead be incorporated into the access requirements, especially R1.3. This will make it clear that in order for someone to be deemed to have access to BCSI, they must have the ability to obtain and use it, which would align with the ERO Practice Guide. Although, we don't recommend using the actual terms "use" and "obtain", without providing more clarification as to their meaning.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
Seattle supports the comments of SMUD to this question.	
Likes 0	
Dislikes 0	

Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
Disagree with the phrase “by eliminating the ability to obtain and use” and it should be moved to Guidelines and Technical Basis to explain what constitute a BCSI access. Agree with adding disposal since it was missing from current CIP-011-2 R1.2. Suggest making the following changes for R1 Part 1.2: “Method(s) to prevent unauthorized access to BES Cyber System Information during, including storage, transit, use, and disposal.” Suggest adding the following language into Guidelines and Technical Basis based on CMEP BCSI Practice Guide: “BCSI access means any instance or event during which a user obtains and uses BCSI. For access to occur, in this context, a user, authorized or unauthorized, must concurrently both obtain BCSI and possess the ability to use BCSI. An unauthorized individual who obtains encrypted BCSI but has no ability to use it within a meaningful timeframe should not be considered to have access.”	
Likes 0	
Dislikes 0	
Response	
Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	

Answer	No
Document Name	

Comment

Xcel Energy support the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Agree with terms “obtain” and “use;” however, more explanation is needed within the requirement or guidelines. The drafting team has referred to the CMEP BCSI practice guide. Recommend defining “BCSI Access” in the NERC Glossary of Terms per the practice guide: “An instance or event during which a user obtains and uses BCSI. For access to occur, in this context, a user, authorized or unauthorized, must concurrently both obtain BCSI and possess the ability to use BCSI. An unauthorized individual who obtains encrypted BCSI but has no ability to use it within a meaningful timeframe should not be considered to have access.”

Disagree and very concerned with the phrase “by eliminating the ability” to obtain and use. This represents an unachievable evidencing threshold over and above the current “Procedure(s) for protecting and securely handling.” Responsible Entities can document protective procedures, but will be hard pressed to prove they have eliminated all ability to obtain and use, i.e. rendered unauthorized access impossible.

Disagree with the addition of “and disposal” to the end of the requirement. BCSI in BES Cyber Systems is already addressed in R3 Part 3.1., but Part 3.1 needs to reinstate the qualifying language in the Requirements “that contain BES Cyber System Information.” Deletion of this qualifying language is an expansion of scope to the current CIP-011-2 R2 requiring evidence of sanitization of assets not containing BCSI subject to this protection.

Although a logical inclusion as part of the lifecycle of BCSI, as applied in R1 Part 1.2, the evidencing we do in R3 for hardware is now going to be extended to the disposal/deletion of BCSI, on every medium, wherever stored, since the Measure calls for “Evidence of methods used to prevent the unauthorized access…” during disposal. The evidencing burden here can be crushing. Example concerns include:

- How will auditors know what BCSI has been disposed of unless Entities maintain an active inventory of BCSI “info items” and status, active or disposed, just like we do for BES Cyber Systems?

- Entity may have a policy to shred paper-based BCSI as the disposal method, but to evidence the method was used, does Entity have to log documents shredded?

- Will every electronic file, document, or email containing BCSI require its deletion to be logged by IT? Will Entities have to obtain such logs from third-party vendors/data custodians?

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 ‘obtain’ and ‘use’ terms are not defined and will lead to additional ambiguity and confusion. It is impossible for entities to know the capabilities of potential threats, ‘use’ from one party may be different than another.

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller

Answer	No
Document Name	

Comment

1. CIP-011 R1, Part 1.2 states “*….by eliminating the ability to obtain and use BES Cyber System Information during storage, transit, use, and disposal*.” Does a format of portable storage media (e.g. flash drives) eliminate the ability to obtain and use BCSI?

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Adding the additional terms of “obtain” and “use” to try to imply the use of encryption without explicitly stating the requirement weakens the language. Further, the use of the word “eliminating” adds significant burden to entities to prove their choosen method can never be compromised. Removal of the phrase “by eliminating the ability to obtain and use BES Cyber System Information” makes the requirement clear and allows entities to select current

and future technologies to protect BCSI during storage, transit, use, and disposal. Consequently, by including these four phases protections for “obtaining” access and during “use” are included in a number of current storage and transit technologies.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy generally agrees that the inclusion of the terms “obtain” and “use” in requirement CIP-011-3, Requirement R1 Part 1.2 will more accurately address the risk related to the potential compromise of BCSI. Duke Energy foresees a challenge to be able to demonstrate how we “eliminate” the ability to “obtain and use” BCSI. Suggest change "eliminating" to "limiting" or "restricting". Insert "both" before "obtain and use".	
Likes 0	
Dislikes 0	
Response	
William Hutchison - Southern Illinois Power Cooperative - 1	
Answer	No
Document Name	
Comment	
Comments: It is impossible to completely “prevent” and or “eliminate” the ability to obtain and or use BCSI during storage, transit, use, and disposal, so all Entities would be in violation the way this is written. The reasons the standards exist are to lower cyber security risks to the BPS. Suggest replacing “eliminating” with “reducing” or rewording the requirement language to: “Method(s) to reduce the risk of unauthorized access to BCSI during storage, transit, use and disposal.”	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colleen Campbell - AES - Indianapolis Power and Light Co. - 3	
Answer	Yes
Document Name	
Comment	
As long as both terms are defined properly, this methodology will help improve the storage of BCSI requirement.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, 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 agrees with the inclusion of the “obtain” and “use”. PG&E recommends that examples of what is “obtain” and “use” be included in the Technical Rationale document to help better understand the intended meaning and to avoid potential future interpretation differences or ambiguities.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	

Comment	
ERCOT believes this is an improvement and provides clarity on the meaning of unauthorized access.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	
However, see other Entities comments related to wording change suggestions	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
This is an improvement and provides clarity on the meaning of unauthorized access.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

OPG is in agreement with RSC provided comment	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	Yes
Document Name	
Comment	
However, see other Entities comments related to wording change suggestions.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NextEra	
Answer	Yes
Document Name	
Comment	
While we agree that “obtain” and “use” more accurately address the risk, we have concerns with the overall wording. We recommend changing Part 1.2 from <<Method(s) to prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BES Cyber System Information during, including storage, transit, use, and disposal.>> To <<Method(s) to prevent the ability to obtain and use BES Cyber System Information through unauthorized access during, including storage, transit, use, and disposal.>> because “eliminating” is an absolute which makes implementation and demonstrating Compliance too challenging.	
Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2	
Answer	Yes
Document Name	

Comment

NYISO feels that “Obtain” and “use” are key distinctions providing clarity related to what is required to prevent unauthorized access. NYISO would also suggest that the following modification be made to the Requirements language:

“Method(s) to prevent unauthorized access to BES Cyber System Information by restricting the ability to both obtain and use BES Cyber System Information during storage, transit, use, and disposal.” In the case where BCSI is encrypted, information could still be obtained (physically or electronically) but would not be in a usable format.

Note – During the Q&A session on the 2019-02: BES Cyber System Information Access Management *webinar (*January 16, 2020*), it appears that “access” equated to having the ability to “obtain and use.” Part 1.2 language seems to be focused on the prevention of unauthorized access by “restricting” the ability to “obtain and use,” NYISO recommends the SDT clarify this point within the Technical Rationale for Reliability Standard CIP-011-3.*

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	

Comment

Yes – somewhat. “Obtain” and “use” are key distinctions which help provide better clarity related to what is required to prevent unauthorized access. In addition, MISO suggests the following modification to the Requirements language:

“Method(s) to prevent unauthorized access to BES Cyber System Information by [delete the word "eliminating"] *restricting* the ability to *simultaneously* obtain and use BES Cyber System Information during storage, transit, use, and disposal.”

Note – based on the Q&A session during the 2019-02: BES Cyber System Information Access Management *webinar* hosted on January 16, 2020*, it appears that “access” equates to having the ability to “obtain and use.”*

As the intent of Part 1.2 is to prevent unauthorized access by “restricting” the ability to “obtain and use,” MISO recommends the SDT clarify this point in the Technical Rationale for Reliability Standard CIP-011-3.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	Yes
Document Name	

Comment

While we understand why “obtain and use” are included in Part 1.2, we fear that the way the requirement is written, the intent will be obscured. For instance, the word “eliminating”, implies perfect execution. This is unattainable and should be avoided in the requirement language. While the changes to this part are a good start, we feel that they are too narrowly focused on cloud-service providers and add extra burden to existing information protection programs.

We encourage the SDT to develop a thoughtful process across all of CIP-011.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	Yes
Document Name	

Comment

Yes the requirement is improved with the suggested terms "use" and obtain". However, the proposed requirement is somewhat circular and should be further improved as follows:

"Method(s) to prevent unauthorized access to BES Cyber System Information during storage, transit, use, sanitization, and disposal." (The inclusion of sanitization here eliminates the need for R3 Part 3.1.)

The term "eliminating" suggests a zero-defect approach, which is an extremely challenging compliance outcome to achieve.

The second bullet in the both R1 Part 1.2 and Part 1.3 Measures is fragmented and introduces topics (e.g. key management program) that have yet to be presented in the standard.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes

Document Name	

Comment

IESO agrees in principle with the comments submitted by NPCC:

While we agree that “obtain” and “use” more accurately address the risk, we have concerns with the overall wording because “eliminating” is an absolute (i.e. zero defect) which makes implementation and demonstrating Compliance too challenging

We recommend changing Part 1.2 from

<<Method(s) to prevent unauthorized access to BES Cyber System Information by *eliminating* the ability to obtain and use BES Cyber System Information during, including storage, transit, use, and disposal.>>

To

<<<<Method(s) to prevent unauthorized access to BES Cyber System Information by *controlling* the ability to obtain and use BES Cyber System Information during, including storage, transit, use, and disposal .>>

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

The ability to “obtain and use” allows for the use of encryption as an acceptable means of protecting BCSI and helps to clarify “knowing and utilizing the information” is what were aiming to protect, instead of simply possessing it. Additionally, Black Hills would like to see “Use” definded in the Glossary.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	Yes
Document Name	

Comment

If you can clean up the sentance better.

Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
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	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	

Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE agrees that this will more accurately address the risk related to the potential compromise of BCSI versus the previous approach. This focus is on the BCSI (data) versus applicable systems that would contain BCSI. This also aligns with the CMEP Practice Guide: ERO Enterprise CMEP Practice Guide BES Cyber System Information. Texas RE does have a concern that entities could simply use the bare minimum controls. For example, a registered entity could comply using encryption, but there is no established brightline criteria indicating what level of encryption is sufficient to meet the objective of this requirement. This may result in inconsistent enforcement of this requirement across the regions. If encryption is to be considered an acceptable means of prevent unauthorized access to BES Cyber System Information then Texas RE recommends that the SDT review NIST Special Publication 800-175B, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms, and incorporate guidance from the NIST publication into the CIP standard where appropriate and applicable. Additionally, in the measures an example of evidence is 'retention in the Physical Security Perimeter.' Texas RE agrees that for BCSI in a physical form retention in a PSP is an adequate means of protection. However, the PSP would not be considered adequate protection for electronic BCSI that is located on a server outside of the Entity's ESP.	
Likes 0	
Dislikes 0	
Response	

5. The SDT is proposing to have BCSI in the "Applicability" column. Do you agree that this provides better clarity on the focus of the requirements?

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller

Answer	No
Document Name	

Comment

Due to strong disagreements with 1.2, 1.4 and R2, we disagree here.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

We can agree with identifying BCSI in CIP-011-3 R1.1 and then using BCSI only in later applicability tables, but cannot support the removal of Medium Impact BES Cyber Systems with ERC.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy support the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	No
Document Name	

Comment
Support the MRO NSRF comments

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	

Comment
Although Seattle finds the proposed approach intriguing, it also finds unnecessarily confusing the inconsistent application of this approach among R1.1-R1.3 and R1.4-1.5, R2, and R3. Better would be to revise the entire Standard one way or the other. Seattle also believes that an objective-based, risk-focused approach would eliminate the need to add “BCSI” to the Applicability column at all. It would be up the entity to specify its own controls in its plan and whether they are controls for BCSI about specific impact ratings of BCS, BCSI storage locations, third party BCSI storage providers, etc.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	

Comment
While having BCSI in the applicability column provides clarity, it unfortunately expands the scope of the requirements beyond what they are today. If the requirements are kept focused on designated storage locations for BCSI, it eliminates confusion with BCSI that may reside in BCS, EACMS and PACS.

We understand that this is a challenging part of the project, but we are concerned that the applicability and associated requirements as currently drafted will create confusion, redundancy and expanded scope. Other than reverting back to the original structure, a possible solution could be to add exclusions to the applicability to exclude High and Medium Impact BCS and their associated EACMS and PACS.

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

What was the intent of stating “BCSI as identified in R1.1”? Is the SDT inferring that other BCSI exists that was not identified in R1.1?

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Black Hills does not think the current definition of BCSI provided in the Glossary is clear enough to allow for BCSI to be listed as an *Applicable System*. We think it would make more sense to leave applicability listed as High and Medium BCS… and state in the requirement “For BCSI, perform action “X,”” as the current CIP-004 R4.1 is modeled, for example.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

AECI supports comments filed by NRECA

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

While NRECA understands what the SDT was attempting to accomplish and does not disagree with the intended clarification, the replacement of "Applicable Systems" with "Applicability" is problematic as such term is already utilized in Section 4 of the CIP-011 standard, and, there, it is utilized to denote whether a registered function has responsibility under the Standard. Utilization of the same term, but with a different scope within body of CIP-011 will result in confusion and ambiguity regarding the overall applicability of CIP-011. Further, this change results in CIP-011 being different from the remaining CIP reliability standards relative to the CIP reliability standards overall approach to identification of asset scope. Finally, NRECA notes that it is also concerned that the modifications to the contents of the "Applicability" column conflict with the definition of BCSI set forth in the Glossary of Terms Used in NERC Reliability Standards. Specifically, the revisions limit the "applicability" to "system information pertaining to…" while 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.

There is information that is not "system information pertaining to" a particular asset that could be used to "gain unauthorized access or pose a security threat to the BES Cyber System." Further, the definition makes explicit reference to "security procedures or security information;" neither of which is confined to "system information" and both of which may be comprised of information that is not "system information." These potential conflicts and contradictions between the standard and the Glossary of Terms Used in NERC Reliability Standards could result in increased ambiguity and confusion.

Finally, NRECA notes that requirement applicability is already complicated and in need of simplification. This modification and addition of the same term within the standard and requirement only serves to increase the complexity and the likelihood for ambiguity and confusion. As well, it must be noted that this change presents a substantial challenge to audit as the implication is that all system information must be evaluated to demonstrate that it was evaluated for identification as BCSI and, further, relative to compliance monitoring activities, all such system information must be available to sample to determine whether the process identified it as BCSI or not. NRECA does not agree that this provides better clarity on the focus of the requirements and, therefore, does not support this change.

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

We disagree with changing the column heading and adding “system information pertaining to” for the following reasons. First, it is inconsistent with other standards and it is confusing to have “applicability” here and also in section A.4 where it lists “Applicability” of functional entities and facilities. Secondly, the definition of BCSI includes information about low impact systems. Therefore, we will be identifying all BCSI in our organization as required by R1 Part 1.1. However, the applicable systems column defines the scope of systems to which the requirement row applies. By referring to “BES Cyber System Information as identified in Requirement R1 Part 1.1” for the applicability of subsequent parts, the scope of systems to which the requirements applied has been increased, since we will have identified BCSI pertaining to low impact systems as well. Third, CIP-011 has always been about BCSI, regardless of where it is stored, so this does not clarify anything further.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

While GSOC understands what the SDT was attempting to accomplish and does not disagree with the intended clarification, the replacement of “Applicable Systems” with “Applicability” is problematic as such term is already utilized in Section 4 of the CIP-011 standard, and, there, is utilized to denote whether or not a particular registered function has responsibility under the Standard. Utilization of the same term, but with a different scope within body of CIP-011 will result in confusion and ambiguity regarding the overall applicability of CIP-011. Further, this change results in CIP-011 being different from the remaining CIP reliability standards relative to the CIP reliability standards overall approach to identification of asset scope. Finally, GSOC notes that it is also concerned that the modifications to the contents of the “Applicability” column conflict with the definition of BCSI set forth in the Glossary of Terms Used in NERC Reliability Standards. Specifically, the revisions limit the “applicability” to “system information pertaining to…” while 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.

There is information that is not “system information pertaining to” a particular asset that could be used to “gain unauthorized access or pose a security threat to the BES Cyber System.” Further, the definition makes explicit reference to “security procedures or security information;” neither of which is confined to “system information” and both of which may be comprised of information that is not “system information.” These potential conflicts and contradictions between the standard and the Glossary of Terms Used in NERC Reliability Standards could result in increased ambiguity and confusion.

Finally, GSOC notes that requirement applicability is already complicated and in need of simplification. This modification and addition of the same term within the standard and requirement only serves to increase the complexity and the likelihood for ambiguity and confusion. As well, it must be noted that this change presents a substantial challenge to audit as the implication is that all system information must be evaluated to demonstrate that it was evaluated for identification as BCSI and, further, relative to compliance monitoring activities, all such system information must be available to sample in

order to determine whether the process identified it as BCSI or not. For these reasons, GSOC does not agree that this provides better clarity on the focus of the requirements and, therefore, cannot support this change.

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	No
Document Name	

Comment

SMEC agrees with comments submitted by NRECA.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

R1.2 - No

R1.3 – Move to R1.5 - these specific requirements should be placed in the appropriate standards CIP-004 and CIP-013.

Likes 0	
Dislikes 0	

Response

Vivian Moser - APS - Arizona Public Service Co. - 3

Answer	No
Document Name	

Comment

AZPS does not agree that the proposed revisions to the “Applicability” column provides better clarity on the focus of the requirements. AZPS requests revising the applicability column to read as follows: “System information pertaining to (but not including the BES Cyber System (BCS) which may contain BCSI):…” or similar language to to clearly establish the focus on BCSI.

Likes 0	
Dislikes 0	

Response

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3

Answer	No
Document Name	

Comment

While having BCSI in the applicability column provides clarity, it unfortunately expands the scope of the requirements beyond what they are today. If the requirements are kept focused on designated storage locations for BCSI, it eliminates confusion with BCSI that may reside in BCS, EACMS and PACS. We understand that this is a challenging part of the project, but we are concerned that the applicability and associated requirements as currently drafted will create confusion, redundancy and expanded scope. Other than reverting back to the original structure, a possible solution could be to add exclusions to the applicability to exclude High and Medium Impact BCS and their associated EACMS and PACS.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

See NRECA submitted comments.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment
We disagree with any and all Applicability that does not include the qualifying language “with ERC” for Medium Impact BES Cyber Systems except for the initial 1.1. The proposed language does not provide more clarity and needs to be more specific, not referencing another part. We recommend going back to ‘Applicable Systems’. Recommendation: All parts of R1 needs to go back to “Applicable Systems”, The “Applicability” for R2, is acceptable. Add clarity to the R2 Applicability with “BES Cyber System Information stored in Vendor managed electronic BCSI Repositories, and pertaining to: (Applicable Systems)“ R3 needs to stay, ‘Applicable Systems’.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
BPA finds the proposed language is a significant change, and entities (and possibly auditors) do not have experience in applying this requirement to information. This may cause some confusion. CIP-011 is an information protection standard and it is sensible to put such a requirement here. Referring to the CIA model of Confidentiality, Integrity, and Availability, cyber security methodology often differentiates between protecting systems functionality/availability, vs. data. It is sometimes desirable to share data while still protecting the system from unauthorized use. If the SDT’s intent is to address distinct protections for data that may be processed, stored, or transmitted by the system separately from configuration information about the system itself (i.e., versions, settings, and runtime parameters), the definition of “Cyber Assets” (NERC Glossary pg. 10) should be examined to further clarify which and to what extent “data in those devices” is subject to which requirement.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	

Comment

Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC	
Answer	No
Document Name	
Comment	
NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES	
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	

We agree it clarifies the focus is on protecting the information, however we disagree that is the right focus for this type of standard. With the focus on BCSI comes the issue that the requirements are now impossible to measure on every piece of BCSI everywhere. It is only measurable at BCSI storage locations or repositories. *See answer to Question 2 for additional explanation.*

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

While providing better clarity it may expands the scope of requirements beyond what are in place today.

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.

Additionally, SDG&E would like to comment on CIP-011-3 requirement's proposed inclusion of all Medium-Impact BCS, regardless of ERC. The current CIP-004-6 R4.4 requirement specifies applicability for only High Impact BCS and Medium Impact BCS with ERC. The new CIP 011-3 brings all BCSI in scope regardless of ERC in Medium-Impact Sites. This change is significant and overburdensome to sites that don't currently fall into this category of BCSI.

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 response found in the NSRF Comment Form	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We disagree with any and all Applicability that does not include the qualifying language "with ERC" for Medium Impact BES Cyber Systems except for the initial 1.1. The proposed language does not provide more clarity and needs to be more specific, not referencing another part. We recommend going back to 'Applicable Systems'. *Recommendation: All parts of R1 needs to go back to "Applicable Systems", The "Applicability" for R2, is acceptable. Add clarity to the R2 Applicability with "BES Cyber System Information stored in Vendor managed electronic BCSI Repositories, and pertaining to: (Applicable Systems)" R3 needs to stay, 'Applicable Systems'.*	
Likes 0	
Dislikes 0	
Response	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
While we understand the reasoning behind the change, we feel that this change adds confusion and inconsistencies between CIP-011 and the rest of the CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support MRO comments.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Please provide more clarity on the phrase "System information pertaining to". This needs to be well defined and understood. There may be many systems that are associated with systems that may or may not house BCSI.	
Likes 0	
Dislikes 0	
Response	

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CEHE supports the comments as submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI supports adding BSCI in the Applicability Column of CIP-011-3. However, there are concerns with expanding the applicability to PCAs and Medium Impact BES Cyber Security Systems. First, in evaluating the proposed revision against the approved SAR, we are unable to find language to support the proposed revision. Second, the SDT should provide support that this modification will alleviate a reliability gap. Specifically, we ask the SDT to provide information regarding the reliability gap the proposed modifications are intended to address. Alternatively, the SDT could study the issue and develop a white paper, to identify, justify and explain the gap that they believe exists and, if necessary, revise the SAR.	
Likes 0	
Dislikes 0	
Response	

Gregory Campoli - New York Independent System Operator - 2	
Answer	No
Document Name	
Comment	
NYISO understands the intent of the change. However, we are concerned that this would create an inconsistency in format with the other current CIP standards. NYISO would propose keeping the original “Applicable Systems” title and adding language such as “System Information pertaining to:” at the head (or similar) of each applicable row in requirements R1 and R2.	
Likes 0	

Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	No
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE agrees with EEI’s comments	
Likes 0	
Dislikes 0	
Response	

Angela Gaines - Portland General Electric Co. - 1	
Answer	No
Document Name	
Comment	
Please see comments PGE Group 2	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
We disagree with any and all Applicability that does not include the qualifying language “with ERC” for Medium Impact BES Cyber Systems, except for R1 Part 1.1, if restricted to identifying BCSI, and the identification of BCSI storage locations, or Repositories, is broken out into a separate part (with Applicability to include “with ERC”) per Q1 response. The proposed language does not provide more clarity and needs to be more specific, not referencing another part. We recommend going back to “Applicable Systems.” Recommendation: All parts of R1 need to go back to “Applicable Systems.” The “Applicability” for R2, is acceptable. Add clarity to the R2 Applicability with “BES Cyber System Information stored in Vendor managed electronic BCSI Repositories, and pertaining to: (Applicable Systems).” R3 needs to stay “Applicable Systems.”	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	

Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

We disagree with any and all Applicability that does not include the qualifying language “with ERC” for Medium Impact BES Cyber Systems, except for R1 Part 1.1, if restricted to identifying BCSI, and the identification of BCSI storage locations, or Repositories, is broken out into a separate part (with Applicability to include “with ERC”) per Q1 response. The proposed language does not provide more clarity and needs to be more specific, not referencing another part. We recommend going back to “Applicable Systems.”

Recommendation: All parts of R1 need to go back to “Applicable Systems.” The “Applicability” for R2, is acceptable. Add clarity to the R2 Applicability with “BES Cyber System Information stored in Vendor managed electronic BCSI Repositories, and pertaining to: (Applicable Systems).” R3 needs to stay “Applicable Systems.”

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

IPC does not agree with the change from “Applicable Systems” (High Impact BES Cyber Systems and their associated: EACMS and PACS, etc.) to “Applicability” (BES Cyber System Information as identified in Requirement R1 Part 1.1) nor any reference other than an “Applicable System” reference in the “Applicable Systems” column. IPC believes the “Applicable Systems” language and approach should remain consistent across all CIP Standards. IPC does not agree that this change provides better clarity on the focus of the requirements; rather, this changes introduces and creates ambiguity and inconsistencies across the CIP Standards.

Likes 0	
Dislikes 0	

Response	
Colleen Campbell - AES - Indianapolis Power and Light Co. - 3	
Answer	No
Document Name	
Comment	
Because the definition of BCSI is left for the most part up to the entity this could lead to confusion during an audit if the auditor has a different interpretation for BCSI.	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
Comments: Specification of information as an undefined category (i.e. “system information”) does not support understanding the intention of the information protections being addressed. The shift to an information protection standard is welcome, but would require some support of identifying types of information and developing some sort of inventory that can allow for concrete demonstration of protections and measures to comply. An entity could use a narrow interpretation of “system information” to overtly restrict what is considered BCSI and minimize the compliance burden at the expense of providing information protections. Since the rest of CIP-011-3 R1 depends on R1.1 identification, this could remove most information relevant to protection of cyber assets from consideration for compliance.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	

No comments

Likes 0	
Dislikes 0	

Response

William Hutchison - Southern Illinois Power Cooperative - 1

Answer	Yes
Document Name	

Comment

Comments: Yes, it would be good to have BCSI in the “Applicability” column. We feel BCSI repositories need to have a significant explanation in the “Guidelines and Technical Basis” section as stated in question 1.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Duke Energy generally agrees that adding BCSI in the “Applicability” column provides further clarity on the focus of the requirements. However, Duke Energy suggests using the High and Medium designations carried with the applicability for consistency throughout the rest of the standards. Also, including the term “system information” in the applicability column and BES CSI in the requirement column may introduce scope ambiguity, particularly, for example, PCA is included in the applicability, but is not included in the NERC Glossary term BES CSI.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	Yes
Document Name	

Comment

Agree with proposing to have BCSI in the “Applicability” column and it is much clearer than the

current version since the CIP-011 requirements actually apply to BCSI rather than BCS and their

assocated cyber assets.

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1

Answer	Yes
Document Name	

Comment

That is fine as long as the Applicability section for R1.1 is worded correctly. We do not support introducing "System information pertaining to" in the applicability section for R1.1. This creates some ambiguity. We believe that the applicability be limited to BCSI.

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3

Answer	Yes
Document Name	

Comment

AEP is in agreement that there is an overall increase in clarity on the focus of the standard. However, we were unable to find a justification for the change within the Technical Rationale and have concerns regarding the need for these modifications.

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	
Yes, it would be good to have BCSI in the “Applicability” column. We feel BCSI repositories need to have a significant explanation in the “Guidelines and Technical Basis” section as stated in question 1.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
The intention is good, and provides greater focus, however, the current proposed requirements still have some ambiguity due to the applicability of Requirement R1 including the BES Cyber System and associated Cyber Asset construct as the target.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	

Comment	
N&ST suggests deleting the word, “System,” thereby changing, “System information pertaining,…” to “Information pertaining,…”	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the proposed change as long as the change is coordinated with Project 2016-02 so there is consistency across all CIP standards.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	Yes
Document Name	
Comment	

Yes. We do agree. But does that mean NERC/FERC will consider the applicability section? They don't consider the applicability section related to CIP-002 IRC 2.11 they and FERC claim that non-BES generation is to be considered when performing a nRP evaluation of a GOP Control Center. The Applicability Section says "All BES Facilities". Why is the other CIP drafting team having to redefine BES in the new IRC 2.12. Is NERC and FERC going to pull a fast one again and say entities need to include non-BES Cyber Information in their BCSI Protection Plans?????

- And BES Means BES not non-BES
- and Facilities mean BES equipment not non-BES equipment
- and GOP's don't have GOP functional obligations for non-BES generation.
- Non-GOPs are doing just fine not providing GOP functional obligation services to non-BES generation and so are GOPs; i.e. neither GOP's and non-GOPs have GOP function obligations to any non-BES generator!. We reserve our GOP services for Generation Facilities (I.e. BES by NERC Glossary definition for Facilities and GOP's provide services to a operate Facilities) not non-BES assets, see definition of GOP in NERC Glossary of Terms.
- According to NERC's March 1, 2019 Standards Process Manual Appendix 3A page 6 last paragraph "The only mandatory and enforceable components of a Reliability Standrd are the (1) Applicability, (2) Requirements, and (3) effective dates.
- What good is the Applicability Section if NERC/FERC are going to ignore it?
-

Likes 0	
Dislikes 0	

Response

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members

Answer	Yes
Document Name	

Comment

Yes. However, consistency is important when defining and using terms. Please pick a single descriptor and use it consistently throughout. e.g. BCSI vs BES Cyber System Information.

Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	

Response

James Brown - California ISO - 2 - WECC

Answer	Yes

Document Name	
Comment	
We agree with the approach. Retitling the column to “Applicability” will be beneficial for all Standards and Requirements to allow for more flexibility. This aligns well with the work of the Project 2016-02 Standard Drafting Team that is also introducing new applicability. There may be future instances where the applicability cannot be limited down to a system.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	

We do agree. But does that mean NERC/FERC will consider the applicability section? They don't consider the applicability section related to CIP-002 IRC 2.11 they and FERC claim that non-BES generation is to be considered when performing a nRP evaluation of a GOP Control Center. The Applicability Section says "All BES Facilities".

- And BES Means BES not non-BES
- and Facilities mean BES equipment not non-BES equipment
- and GOP's don't have GOP functional obligations for non-BES generation.
- Non-GOPs are doing just fine not providing GOP functional obligation services to non-BES generation and so are GOP. We reserve our GOP services for Facilities nor non-BES assets.
- According to NERC's March 1, 2019 Standards Process Manual Appendix 3A page 6 last paragraph "The only mandatory and enforceable components of a Reliability Standrd are the (1) Applicability, (2) Requirements, and (3) effective dates.

What good is the Applicability Section if NERC/FERC are going to ignore it?

Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	

Comment
ERCOT agrees with this approach. Retitling the column to “Applicability” will be beneficial for all Standards and Requirements, and allow for more flexibility. This revision aligns well with the work of the Project 2016-02 Standard Drafting Team that is also introducing new applicability. There may be future instances where the applicability cannot be limited down to a system.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: James Mearns, 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 agrees with the Applicability change to “System Information pertaining to” is appropriate and provides clarity on what is to be protected. PG&E has concerns about the addition of PCA to the “System Information” to be protected. The concern is the additional effort to identify and protect this information and the potential benefit of those additional protections. PG&AE is requesting the SDT articulate the reason for the proposed addition of PCA since there is no information in the Technical Rationale document to warrant its addition.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 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	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 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	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
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	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NextEra	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	
Document Name	
Comment	
Neither agree nor disagree	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	

See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	

6. The SDT is proposing to address the security risks associated with BCSI environments, particularly owned or managed by vendors via CIP-011-3, Requirements R1, Part 1.4, and Requirement R2, Parts 2.1 and 2.2. Do you agree that these requirements will promote a better understanding of security risks involved while also providing opportunities for the Responsible Entity to address appropriate security controls?

Bradley Collard - SunPower - 5	
Answer	No
Document Name	

Comment

How are entities to list NERC, Regional Entities, FERC, etc.? The Standard should allow certain exemptions. They should also allow for exemptions post NERC Exceptional Circumstance incidents where the information may be shared to expedite recovery.

Agree with Tarantino's comment about this needs to be included in CIP-013.

Likes 0	
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	

Comment

Comments:

Requirement R1

The language in R1.4 goes beyond providing an opportunity for a Responsible Entity to address appropriate security controls because it requires remediation and mitigation actions, including planned date of completion and status on action items. The requirement should also note that the risk assessment is only necessary when a vendor or other third-party is housing the information. In other words, the assessment should not be required if the information is stored by the Responsible Entity on its premises.

Additionally, the CIP-011 requirements seem to toggle from objective-based requirements to prescriptive-based implementation activities in an unstructured manner. For example: R1.3 (Process to authorize access to BCSI) is objective-based, but R1.5 (Revoke the individual's current access to BCSI by the end of the next calendar day following the effective date of the termination) is prescriptive-based. R1.5 also implies that the process to authorize access to BCSI must be on an individual (person by person) basis, which brings us right back the issue with CIP-004 and having BCSI in the Cloud when an Entity may not have a list of individuals with access to the information. An Entity should be able to authorize a company, vendor, individual, etc. to access information and it should have the flexibility to define how it implements the authorization process.

Requirement R2

The Standards should remain technology neutral. By prescribing key control management programs, there is an assumption that key management is the only way to address preventing the ability to obtain and use BCSI through unauthorized access. Again, the requirements toggle between objective-based and prescriptive/technology-based.

Recommendation: the SDT should consider either including information protection measures for vendors in CIP-013, or approaching CIP-011 similarly to CIP-013. Specifically, the SDT should consider creating a requirement to develop and implement a BCSI security risk assessment plan and describe the criteria that should be included in the plan (for example, a process to authorize access, a process to prevent ability to obtain and use BCSI from unauthorized access, a process to revoke access within the next calendar day, etc.). This approach allows an Entity:

- to focus on identifying information security risks and objectives specific to its needs and appropriately addressing them;
- flexibility and scalability regarding how to implement technical controls, as well as remediation & mitigation activities; and
- the ability to leverage emerging technologies that might better address information security risks without requiring updates to CIP Reliability Standards.

Likes 0	
Dislikes 0	

Response

Colleen Campbell - AES - Indianapolis Power and Light Co. - 3

Answer	No
Document Name	

Comment

The way the requirement is currently written there is confusion between how R2 will be applied to on premise storage solutions. The “Where Applicable” reference does not fully explain the types of storage locations referred to in the requirement.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

We believe R1 Part 1.4, and R2 Parts 2.1 and 2.2, exceed the scope of the SAR. We agree with EEI comments that vendor risk assessments with respect to hosting BCSI should be addressed with a modification to CIP-013.

We concur with EEI comments that the draft requirement R2.1 regarding key management is unclear, and yet, at the same time, too prescriptive.

Similar to the explanation of the term “vendor(s)” in the CIP-013 Supplemental Material, it must be made clear with respect to vendors in R1 Part 1.4, and custodial entity in R2 Part 2.2, that Regional and Registered Entities, as well as NERC and FERC, are exempted as such.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: James Mearns, 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 agrees that R1 P1.4 and R2 are a good start in addressing the security risks of BCSI but is concerned with the apparent overlap that P1.4 has with CIP-013 Supply Chain Risk Management R1 P1.1 risk assessment. Could CIP-011 SDT just reference the CIP-013 requirements for vendor risk assessment and allow the entity to determine the appropriate method(s) for determining the risk, documentation of the risks and frequency of re-assessment based on their CIP-013 plan(s)?

PG&E also has a concern regarding the language of Requirement R2. PG&E believes that it is not clear if key management is for physical, electronic, or both types of keys. This lack of clarity could lead to entity confusion on what is covered. The Technical Rationale document for Requirement R2 does indicate it covers both, but we are aware the Technical Rationale document is not always read and does not carry the same compliance mandate as Requirement language.

PG&E recommends the Requirement language clearly indicates key management should cover such items as physical and electronic keys, with the “such as” proceeding the “such as” to possibility future proof the Requirement to technology changes we are not aware of yet.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.

Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Regarding Part 1.4, this requirement appears to be better addressed in CIP-013. ERCOT refers the drafting team to ERCOT's comments in response to Question No. 3 recommends excluding applicability of all requirements for cloud service providers, but including the minimum requirements in the cloud vendor risk assessments of Part 1.4.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
We believe R1 Part 1.4, and R2 Parts 2.1 and 2.2, exceed the scope of the SAR. We agree with EEI comments that vendor risk assessments with respect to hosting BCSI should be addressed with a modification to CIP-013. We concur with EEI comments that the draft requirement R2.1 regarding key management is unclear, and yet, at the same time, too prescriptive. Similar to the explanation of the term "vendor(s)" in the CIP-013 Supplemental Material, it must be made clear with respect to vendors in R1 Part 1.4, and custodial entity in R2 Part 2.2, that Regional and Registered Entities, as well as NERC and FERC, are exempted as such.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	

Comment
This is way too prescriptive. Vendor requirements should reside only in CIP-014.

Likes 0	
Dislikes 0	

Response

Angela Gaines - Portland General Electric Co. - 1	
Answer	No
Document Name	

Comment
Please see comments PGE Group 2

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	No
Document Name	

Comment
While the proposed changes to promote a better understanding of the security risks, they are not in alignment with the current CIP-013-1 Standard for Supply Chain Risk Management. Third-parties are part of the supply chain, and adding a Supply Chain Risk Management (SCRM) requirement within CIP-011-2 R1 Part 1.4 adds unnecessary ambiguity and double jeopardy with Cloud Providers SCRM requirements falling under both CIP-013-1 and CIP-011-3. Additionally, the R2 requirements add additional ambiguity in their applicability. R2 Part 2.1 has a “where applicable” clause which seems to alleviate the compliance burden for an entity that does not use PKI or like key management. Part 2.2 does not have this “where applicable” clause, but relies on duties identified in Part 2.1, which would still apply to an entity without PKI, but what are the compliance requirements in this case? Additionally, R2 imposes a significant burden on an entity who has key management infrastructure and local only BCSI storage. If there is key management infrastructure at the enterprise level, this does not mean that the entity is capable of implementing this infrastructure to encrypt local BCSI storage locations using the PKI, nor is there a requirement to do so. However there would be a requirement to implement documented processes supporting R2 for an infrastructure that has no relevance to the BCSI.

A possible solution to this issue would be to modify the applicability to “BCSI from R1 Part 1.1 that is encrypted using a key management infrastructure” or similar.

OR to change the R2 level language to something similar to this:

“Each Responsible Entity shall implement one or more documented key management programs that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection, for key management infrastructure used to protect BCSI. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].”

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2

Answer	No
Document Name	

Comment

PGE agrees with EEI’s comments

Likes 0	
Dislikes 0	

Response

James Brown - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

Regarding Part 1.4, this requirement appears to be better addressed through CIP-013. Please see comments to question #3. Recommend to exclude applicability of all requirements for cloud service providers and include the minimum requirements in the cloud vendor risk assessments of R1.4.

Likes 0	
Dislikes 0	

Response

Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF

Answer	No

Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI's comments. Specifically, if key management is not a requirement (due to the "where applicable" language in 2.1), then it is not appropriate to have this language in the requirements section and would be better suited to guidance. The requirements should only state what is required.	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
SNPD supports the fundamental requirements and reasoning behind the proposed additions but believe it would be better placed within the context of CIP-013 vendor and supply chain risk management. CIP-011 should be limited to information handling and protection. Vendor vetting and management would appear to fit better within the overall context of CIP-013.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
This is way too prescriptive. Vendor requirements should only reside in CIP-014.	
Likes 0	
Dislikes 0	
Response	
Gregory Campoli - New York Independent System Operator - 2	

Answer	No
Document Name	

Comment

If the intent of the proposed changes to CIP-011-3, requirement R1, Part 1.4 is to better understand and mitigate assessed risks to BCSI being stored within a vendor-managed environment, NYISO believes the proposed changes are potentially overly broad and administratively burdensome in comparison to risks currently assessed under CIP-013-1.

As stated in our response to question #3, NYISO would recommend eliminating Part 1.4 of requirement R1 from CIP-011-3. The issue of risk assessments for vendors could be addressed as part of Project 2019-03: Cyber Security Supply Chain Risks (i.e. CIP-013-2), this would have the benefit of accounting for all vendor requirements (BCS and BCSI) within the same standard.

Regarding examples contained within CIP-011-3, requirement R2, Parts 2.1 and 2.2, a key management process is an example of one method that could be applied to prevent unauthorized access. NYISO feels that this example would be better included under requirement R1. NYISO proposes requirement R2 be removed from the current draft.

Another suggested consideration would be include protections of BCSI stored in environments owned or managed by third parties into a separate requirement. For example, combine the requirements into “R4”, which could reference R2 (Key management) as a stated requirement (not optional) for BCSI stored in environments owned or managed by third parties.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

There are other more appropriate methods to “promote better understanding” of issues and topics than through the standards drafting process. Perhaps such issues and topics could be included as part of a Technical Rationale, supporting white paper, or using other available mechanisms.

With regard to CIP-011-3, Requirement R1, Part 1.4, the requirements appear to duplicate CIP-013 Requirements. As such, we would encourage the SDT to address a perceived security gap of BCSI stored at third party facilities within the CIP-013-1 Standard.

Regarding CIP-011-3, Requirement R2, Parts 2.1 and 2.2; EEI offers the following comments:

The SDT is prescribing requirements that do not appear to conform to NERC guidance regarding development of results-based Reliability Standards. While encryption and key management would be an acceptable method for ensuring the security of BSCI at third party facilities, specifying this solution within requirements may be overly prescriptive and potentially limit entities from using other methods to secure BCSI, if future technology advancements offer such solutions. For this reason, the language should be broader with less prescription. If the SDT believes that the requirements as described in R2 must be pursued, EEI suggests the following:

Part 2.1: “Where applicable” should be more clearly defined in order to avoid any confusion as to when key management processes are required, otherwise the list of processes appears to be sufficiently comprehensive to ensure the security of BSCI.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

If the SDT’s intent is to address security risks associated with vendors, then that should be specifically expressed in the requirements. The current language is vague and needs further clarification. Part 1.4 states “in cases where vendors store” but Part 2.1 and Part 2.2 do not. In Part 2.1, the statement “where applicable” needs to be expanded to clearly provide when a key management program must be implemented. As written, the proposed requirements are too broad and could add an undue burden if auditors take the broadest possible meaning. Part 2.2 is not clear due to the vagueness of Part 2.1. The following changes are suggested;

“Part 2.1 When BCSI is stored in environments owned or managed by vendors, develop a key management process(es) …”

“Part 2.2 When BCSI is stored in environments owned or managed by vendors, implement controls to separate …”

Also in reference to Part 2.2, the phrase “BCSI custodial entities duties” is not clear and open to broad interpretation.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	

Comment

No – if the intent of the proposed changes to CIP-011-3, requirement R1, Part 1.4 is to mitigate risks particular to BCSI stored in a vendor managed environment, MISO believes the proposed changes are overly broad and administratively burdensome in comparison to those risks currently assessed under CIP-013-1 and the small amount of incremental benefit gained in relation to the level of effort required to produce it.

MISO recommends eliminating Part 1.4 of requirement R1 from CIP-011-3 and recommends the issue of risk assessments for vendors be addressed as part of Project 2019-03: Cyber Security Supply Chain Risks (i.e. CIP-013-2), thereby covering all vendor requirements (BCS and BCSI) in the same standard.

Regarding proposed CIP-011-3, requirement R2, Parts 2.1 and 2.2, a key management process is an example of one method to prevent unauthorized access and would be better included as an example under requirement R1. MISO proposes requirement R2 be eliminated altogether.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support MRO comments.	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
To avoid confusion and the splitting of requirements, vendor risk management, including risk assessments of vendors, should be included in CIP-013. Additionally, the concept of assessing the risk of cloud-providers is good, but the execution within the requirements needs more work. For instance, the requirement is unclear on what constitutes a vendor “storing” an entity’s BCSI, and an auditor could make the assumption that this requirement applies to all vendors and systems and not just to cloud providers. Another example is the timeframe described in Part 1.4.2. This timeline implies that BCSI is more important than the actual BES Cyber Assets themselves (as CIP-013 has no timeframe for reassessments).	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	

Comment

1. We have strong apprehensions on “mitigate” in Part 1.4 and possibly push some to vote NO on this project. See #2 for more feedback. NYPA is voting ‘NO’ based on these apprehensions.
2. We agree with that Part 1.4 will promote a better understanding the security risks involved. We have serious concerns with these controls. Entities have little control of vendors OR the vendors of the primary vendors. We recommend the path laid out by CIP-013 – a) have a plan and b) implement that plan. The potential costs of these controls may not produce an effective result. Plus the submitted feedback to Standards Efficiency Review tends to question the value of annual reviews for the sake of a review instead of a trigger.
3. We request this SDT consider if these vendor controls (mitigations) belong in CIP-013.
4. We request clarification of physical security - will Part 2.2 be difficult to implement where the custodian and the person with the key are the same?

Likes 0	
Dislikes 0	

Response

Ayman Samaan - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

We believe R1 Part 1.4, and R2 Parts 2.1 and 2.2, exceed the scope of the SAR. We agree with EEI comments that vendor risk assessments with respect to hosting BCSI should be addressed with a modification to CIP-013.

We concur with EEI comments that the draft requirement R2.1 regarding key management is unclear, and yet, at the same time, too prescriptive.

Similar to the explanation of the term "vendor(s)" in the CIP-013 Supplemental Material, it must be made clear with respect to vendors in R1 Part 1.4, and custodial entity in R2 Part 2.2, that Regional and Registered Entities, as well as NERC and FERC, are exempted as such.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	No
Document Name	

Comment

1. We agree with that Part 1.4 will promote a better understanding the security risks involved. We have serious concerns with these controls. Entities have little control of vendors OR the vendors of the primary vendors. We recommend the path laid out by CIP-013 – a) have a plan and b) implement that plan.
2. We request this SDT consider if these vendor controls (mitigations) belong in CIP-013.
3. We request clarification of physical security. Part 2.2 may be difficult to implement where the custodian and the person with the key are the same.

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 response found in the NSRF Comment Form

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	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
The BCSI should be protected regarless where it is. When and how to perform risk assessments of the vendors that store the Responsible Entity's BCSI should not become an extra burnden on Responsible Entity.	
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	
R1.4: Southern believes the wording "Process(es) to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information" is less clear. This has no wording to scope it to off-premise situations. Vendors produce all types of data storage solutions and this could be interpreted to mean that all BCSI is stored by a vendor. The requirement should specify the relationship the vendor has to the "storing" of the data as we believe this is about when vendors own/operate/maintain the storage in an off-premise cloud service environment. R2: Requires that an entity "**shall implement** one or more documented key management program(s) that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection" regardless of whether or not an entity encrypts its BCSI or not. For entities that keep all BCSI on-premises and choose to not use 3rd party cloud solutions or encryption as a technical control, this main R requirement serves no purpose, and results in a documentation exercise to 'prove the negative.' Consider moving the term "where applicable" to the main R requirement to explicitly exempt those entities that do use encryption as a technical control to protect BCSI in storage, transit, or use.	

Overall, Southern believes that the R2 requirements for VRA's should be part of CIP-013 which is a more holistic approach to vendor risk. We do not agree with the need to piecemeal different flavors of VRAs throughout the CIP standards for individual technical areas. CIP-013-1 R2 currently has language containing a cyber security risk management plan for supply chain. We suggest this be removed from the proposed CIP-011 and instead be coordinated with the Supply Chain SDT to add language or a requirement to align with conducting vendor risk assessments.

Part 1.4 seems to be somewhat a duplication of 1.6 where a verification of access to BCSI is required on the same time interval.

Likes 0	
Dislikes 0	

Response

Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC

Answer	No
Document Name	

Comment

NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren agrees with and supports EEI comments.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	
Comment	
Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments. Supply chain related related requirements should remain as part of the CIP-013 planning process.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
“System Information Pertaining to” BCS is far too vague. The NERC Glossary definition of BCSI shows examples rather than a principle by which to designate BCSI. Guidance on this point fails to approach data “classification” or “categorization” according to sound and well-developed principles in widespread use for which expertise and guidance exists from the Intelligence community. One vital concept is aggregation of data leading to increased risk. The glossary definition gives an example or hints at it through the phrase “collections of network addresses:” but doesn’t explain how an Entity would create a guideline for policy that assesses risk based on aggregation, doesn’t discuss “Essential Elements of (Friendly) Information” concepts and doesn’t discuss derivative classification and marking.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We believe R1 Part 1.4 and R2 Parts 2.1 and 2.2 exceed the scope of the SAR. Vendor risk assessments are addressed in CIP-013. The result of identifying, assessing, and mitigating vendor risks is still going to be controls we implement to prevent unauthorized access, which is already required in various other current CIP Standards. The concern is that the SDT is developing a requirement that is duplicative of requirements contained within CIP-013, and any modifications should be addressed in that Standard, not in CIP-011-3.	

If R1 Part 1.4 needs to be pursued in CIP-011, per the definition of a Vendor in CIP-013, Regional and Registered Entities, need to be exempted from being regarded as vendors, suppliers, or custodial entities.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST believes that, following the Effective Date of 7/1/20 for CIP-013, vendors offering BCSI storage services will be subject to that Standard, which in our view renders proposed CIP-011-3 Requirement R1, Part 1.4 redundant. Moreover, the proposed requirement is more stringent than any requirement in CIP-013! The SDT is, in essence, proposing to require Responsible Entities to perform ANNUAL vulnerability assessments of their cloud storage vendors (if any). N&ST admits to being hard-pressed to imagine how a Responsible Entity could perform a credible “risk assessment” of, for instance, Microsoft Azure beyond asking them in writing if they still have the same FedRAMP authorization level as they had the previous year. The “Technical Rationale for Reliability Standard CIP-011-3” includes a statement, “If the focus is protection of BCSI, the device or storage location becomes less relevant,” that seems inconsistent with the proposed “risk assessment” requirement. N&ST recommends that it be dropped.

With regards to proposed Requirement R2, Parts 2.1 and 2.2, N&ST considers them vastly over-prescriptive. The goal here is to ensure that no individuals who manage BCSI storage, whether in the Responsible Entity’s own data center or “in the cloud,” can access BCSI unless they have been properly authorized in accordance with the requirements of CIP-004. Encryption and key management are certainly viable options, but they should remain options. N&ST suggests moving them to the “Measures” associated with an appropriately re-worded requirement.

Likes 0	
Dislikes 0	

Response

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3

Answer	No
Document Name	

Comment

While Tri-State G&T agrees with the concept of performing a risk evaluation (proposed by Part 1.4) associated with a cloud solution, we do not agree it needs to be a compliance requirement. We think that the other requirements (access management, methods to protect/secure BCSI, etc.) already force the Registered Entity to evaluate and identify risks, possible solutions, etc. Making the risk evaluation a mandatory requirement does not add value, and instead adds unnecessary adminstrative compliance burden.

The R2 requirements as drafted are entirely too prescriptive and should instead be converted to objective-based requirements. Furthermore, as to R2.2, entity’s should be permitted to have the same vendor manage the keys and hold the encrypted data, as long as controls are in place to prevent

unauthorized access and detect when an unauthorized action has been taken. Additionally, the use of the phrase “Where applicable” should be clarified. We recommend instead using the phrase “Where encryption is utilized as a method to restrict access to BCSI”.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

The proposed language for CIP-011-3, Requirements R1, Part 1.4 are not only duplicative of CIP-013, they also prescribe mandatory timeframes for the performance of periodic risk assessments for what is otherwise an objective based standard in CIP-013. This periodicity should be left up to each Registered Entity to define within their Supply Chain Risk Management plan. To remove double jeopardy, prevent confusion, and maintain consistency for supplier risk management requirements, CIP-011-3, Requirements R1, Part 1.4 should be removed and cloud-based suppliers for BCSI should be covered in CIP-013.

Likes 0	
Dislikes 0	

Response

Vivian Moser - APS - Arizona Public Service Co. - 3

Answer	No
Document Name	

Comment

AZPS agrees that the proposed language in Part 1.4 addresses security risks associated with instances where a vendor stores a Responsible Entity’s BCSI. However, Parts 1.4.1 through 1.4.3 introduce duplicative requirements to perform risk assessments, as the requirement will be satisfactorily met with the implementation of CIP-013-1 Part 1.1. AZPS recommends retaining Part 1.4 and remove sub-parts 1.4.1 through 1.4.3.

With respect to CIP-011-3 R2, AZPS provides its response in Question No. 8.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

Requirement R1 Part 1.4 is a step in the right direction for structuring a framework that considers third-party providers as a viable source. However, as written, the language falls short in the following wasy:

- This entire process should be included in the CIP-013 Supply Chain standard that already deals with bendor risk assessments, etc. This is duplicative to that effort and one that would likely be collapsed into CIP-013 during a subsequent efficiency review
- The intent to mitigate risk does not include the intended risk threshold or objective. If this is to be determined by the entity, the outcome should be clearly indicated. If this risk analysis were included in CIP-013, the entity already defines the process and risk objectives there, so this would also be a duplication.
- Part 1.4.3 - is it necessary to state that the entity needs to "document the results of the risk assessment"? This serves as a Measure to Part 1.4.2 than a standalone requirement, which in and of itself, is administrative. Furthermore, Part 1.4.3 should be reworded to state, "Implement an action plan to remediate or mitigate risk(s) identified in the risk assessment performed according to Parts 1.4.1 and 1.4.2, including the planned date of completing the action plan and the execution status of any remediation or mitigation action items."
- Bullets 3 and 4 in the Measures - what is the difference between the "documentation of the vendor risk assessments" and "documentation of the results of the vendor risk assessments"? It seems these could be combined into a singular measure.

With respect to R2 Parts 2.1 and 2.2:

- The objective is to restrict access but it is not clear to what? The requirement should be clarified. Is the key management process intended for physical access to locations of BCSI storage locations? Electronic access to folders and/or information containing BCSI? Both? Something else? This appears to be an available Measure to meet Part 1.2 and not an independent requirement covering the same reliability objective of preventing unauthorized access.
- There are several terms included in the Parts 2.1.1 - 2.1.9 list that are not commonly understood without further explanation (e.g. key suppression, periods). These need to be presented or explained more clearly to inform the Registered Entity what the intent is.
- In Part 2.2, the use of "custodial entity" is not well understood. Furthermore, the intended security objective of this requirement is not clear as a result.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

These additional requirements should be added to the language of CIP-013 and addressed in the entities supply chain risk management plan. Do not mix the standards requirements.

Likes 0	
Dislikes 0	

Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Yes, agree that a stand alone requirement where a vendor stores an entitiy's BCSI is needed. 1.4.1 requires an initial risk assessment of vendors but the SDT needs to define what is acceptable evidence for a risk assessment. Is requirement 2 only applicable to BCSI stored in the cloud? For R2.1 the SDT should define key management and provide guidance in a GTB. For R2.2 if an entity uses secure thumdrives, how can they separate the duties? Who in this requirement is the custodial entity?	
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	
Doing a risk assessment of an 3rd party / offsite storage provider is practically useless. The best a RE will get from most providers is a SOC1 or SOC-2 report. The way this is written today only creates compliance risk and burden on the RE. The majority of offsite/Cloud provider storage solutions (a majority if not all the providers RE's would use) are not the issue when it comes to security risks. These types of businesses would not be in business if they did not have strong security systems in place and would not be used by Federal, State, Local governments and Fortune ranked companies. Instead of putting the burden on the RE, NERC/FERC needs create an approval process and keep an approved published list of 3rd party storage vendors list for RE's to be able to use. This is exactly what is done for government and government contractors. This would be more efficient, more in-depth, and not create compliance burden on the RE's. This would not restrict competition or violate any laws as any 3rd party would be able to go through the process to get approved. In almost all documented cloud data breach cases we are aware of, it has been the end user which has caused data leaks not the provider themselves ref: https://www.wsj.com/articles/human-error-often-the-culprit-in-cloud-data-breaches-11566898203 . We followed this article up by asking various cybersecurity experts from EY, Mandiant, and Cisco. The only compromise which came up from them was 3rd party identity providers. The compromise was of their own outward facing application and not the security of or compromise of customer storage solutions. The greater risk in cloud/3rd party storage solutions lies more in a customer not having the knowledge of the risks and security tools necessary to protect data in the cloud than the cloud provider itself. This is also significantly dependent on the type of environment being used such as a completely private cloud vs hybrid public/private cloud and its subsequent configuration	
Likes 0	

Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC agrees with comments submitted by NRECA.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
GSOC agrees that the proposed revisions will promote a better understanding of security risks involved while also providing opportunities for the Responsible Entity to address appropriate security controls; however, it does not support the manner in which the proposed requirements do so. Specifically, GSOC is concerned about introducing a separate vendor risk assessment for vendors under CIP-011 than is proposed in CIP-013. Such segregation of similar and potentially related requirements and processes into 2 different standards introduces (rather than reduces) overall risk as discussed below in GSOC's response to question #10. If a risk assessment for a vendor is necessary, then, the team should work with the Supply Chain SDT to modify CIP-013. This is especially important where cloud services are provided under a master or general services agreement that is in scope for CIP-013 as an additional requirement under CIP-011 creates redundancy and the potential for error. Further GSOC notes that mitigations are not required to be implemented in CIP-013, but are required to be implemented here for what is likely a less risky procurement. It is unclear as to why this would be necessary and, as this is not addressed within the Technical guidance, it should be addressed by the SDT to ensure that there is an appropriate identification of risk associated with the recommendation to require a separate risk assessment and mandatory risk mitigation within CIP-011 for access to information when mandatory mitigation is not required within CIP-013.	
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
R1 Part 1.4 and R2 Parts 2.1 and 2.2 exceed the scope of the SAR and significantly increase the compliance obligations. CIP-011 should remain non-prescriptive and allow entities to implement the controls appropriate to their situations. Vendor risk assessments are addressed in CIP-013 and should not be required here. In any case, the end result of identifying, assessing, and mitigating vendor risks is still going to be the controls we implement to try and prevent unauthorized access, which is already required by CIP-011. It is also unclear as to when/if these requirements are applicable.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	

Comment
NRECA agrees that the proposed revisions will promote a better understanding of security risks involved while also providing opportunities for the Responsible Entity to address appropriate security controls; however, it does not support the way the proposed requirements do so. Specifically, NRECA is concerned about introducing a separate vendor risk assessment for vendors under CIP-011 than is proposed in CIP-013. Such segregation of similar and potentially related requirements and processes into 2 different standards introduces (rather than reduces) overall risk as discussed below in NRECA's response to question #10. If a risk assessment for a vendor is necessary, then, the team should work with the Supply Chain SDT to modify CIP-013. This is especially important where cloud services are provided under a master or general services agreement that is in scope for CIP-013 as an additional requirement under CIP-011 creates redundancy and the potential for error. Further, NRECA notes that mitigations are not required to be implemented in CIP-013, but are required to be implemented here for what is likely a less risky procurement. It is unclear as to why this would be necessary and, as this is not addressed within the Technical Rationale, it should be addressed by the SDT to ensure that there is an appropriate identification of risk associated with the recommendation to require a separate risk assessment and mandatory risk mitigation within CIP-011 for access to information when mandatory mitigation is not required within CIP-013.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	

Comment

AECI supports comments filed by NRECA	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3	
Answer	No
Document Name	
Comment	
Regarding CIP-011, Requirement 1, Part 1.4, AEP feels that this requirement does not belong in CIP-011. We believe vendor management/supply chain requirements belong in CIP-013 rather than CIP-011. If the current language in CIP-013 does not address BCSI protection when stored at a third party location, AEP recommends modifying the CIP-013 standard to address these needs. In regards to CIP-011, Requirement 2, Parts 2.1 and 2.2, AEP is of the opinion that key management and encryption may not be enough to properly ensure the protection of BCSI when being stored in a third party facility. We also feel these requirements could use some clarification regarding when it's necessary to use key management methods. AEP is unsure of how "where applicable" is defined within Part 2.1, which could lead to insufficient protection of BCSI based on how that phrase is interpreted.	
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 focus needs to be on protecting access to the information. This should be performed in a vendor/platform neutral manner - whether the systems are administered by in-house personnel or hosted on a shared cloud-based hosting provider, the outcome, regardless, should be that access to the information is limited to authorized individuals only. The risk assessment is an additional undue burden on the entity that the existing process should account for regardless of the outside party the information is being shared with. As such, suggest re-architect the standard to be outcome based so as not to preclude using specific technologies or adoption of emergent solutions, and to apply regardless of the outside party with whom the information is shared.	
Likes 0	
Dislikes 0	
Response	

Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

While Tri-State agrees with the concept of performing a risk evaluation (proposed by Part 1.4) associated with a cloud solution, we do not agree it needs to be a compliance requirement. We think that the other requirements (access management, methods to protect/secure BCSI, etc.) already force the Registered Entity to evaluate and identify risks, possible solutions, etc. Making the risk evaluation a mandatory requirement does not add value, and instead adds unnecessary adminstrative compliance burden.

The R2 requirements as drafted are entirely too prescriptive and should instead be converted to objective-based requirements. Furthermore, as to R2.2, entity's should be permitted to have the same vendor manage the keys and hold the encrypted data, as long as controls are in place to prevent unauthorized access and detect when an unauthorized action has been taken. Additionally, the use of the phrase "Where applicable" should be clarified. We recommend instead using the phrase "Where encryption is utilized as a method to restrict access to BCSI".

Likes 0	
Dislikes 0	
Response	

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	

Seattle is concerned about the overlap and potential for conflict between proposed CIP-011 vendor controls and CIP-013. Seattle prefers an objective-based, risk-focused approach that would leverage CIP-013 controls without restating them. Depending on how an entity used, transports, and stores its BCSI, additional controls might be warranted for third parties involved in BCSI processes, but these might be better left up to each entity to determine and defend, based on existing security concepts. For example, an entity may determine that a third-party with a valid FedRAMP certification is sufficiently risk-free to engage to store BCSI, or it might identify specific individual controls. Leaving it up to each entity, with some reasonable guidance, serves to break the Gordian Knot of third-party certifications that to date has stifled most NERC approaches to third party storage providers.

Likes 0	
Dislikes 0	
Response	

Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	

Comment
The requirement language is not clear as SDT expected. If it is intended that R1 Part 1.4 and R2 only apply when vendors are involved, the Requirement language should clearly state this. In addition, for R1 Part 1.4 and R2 Part 2.2, Regional and Registered Entities, as well as NERC and MRO, need to be exempted from any possibility of being regarded as vendors or custodial entities. R2 requires entities to have a key management program, but the wording regarding encryption and vendors are missing. Suggest adding the following language to R2: "… shall implement one or more documented key management program where vendors are custodians and BCSI are encrypted…" In R2 Part 2.1, we believe "key suppression" is a typo and it should be "key supersession". Also if it is intended to address the electronic key rather than physical key, it should clealy state electronic key or encryption key in the requirement language. In R2 Part 2.2, what does the term "custodial entity" mean? If this is a term taken from other guidance or standard documents (NIST, Cloud Security Alliance etc.), those should be referenced. Across various NIST and CSA documents, the terms "data custodian" and "key custodian" are both in use. In R2 Part 2.2, when separation of duties is being called for, it's not clear which particular duties must be kept separate. Also it is not clear whether the separation of duties means between the vendors and Registered Entities. In R2 Part 2.2, it is not clear if it is acceptable for a vendor to have both custody of data and ability to use it (e.g. have an encryption key.) if the vendor separate their staff's duties.

Likes 0	
Dislikes 0	

Response

Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	No
Document Name	

Comment
Support the MRO NSRF comments

Likes 0	
Dislikes 0	

Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
The language appears that the key management would be outside of the Responsible Entity. The Responsible Entity may manage their own keys in certain architectures. Clarification that separations are needed where an vendor (3rd party) is used for key management.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy support the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
The draft requirement R2.1 regarding key management is unclear, and yet, at the same time, too prescriptive. Key management should not be specified as the means, as there are others. R2 Part 2.1 should be deleted in its entirety. Also, for R1 Part 1.4 and R2 Part 2.2, Regional and Registered Entities, as well as NERC and FERC, need to be exempted from any possibility of being regarded as vendors or custodial entities.	

R1 Part 1.4 and R2 Parts 2.1 and 2.2 exceed the scope of the SAR. We do not believe this is an appropriate place to promote better understanding of security risks involved, nor do we think we should be held to these extremely prescriptive requirements. Identifying, assessing, and mitigating vendor risks will already be addressed as part of preventing unauthorized access.

How a Responsible Entity chooses to implement their access control program should not be prescribed within standard language. We suggest removing all language from CIP-011-3 R1.2, R1.4, R2.1 and R2.2. We believe that the inclusion of storing BCSI with cloud based service providers can be addressed by defining “BCSI Access” in the NERC Glossary of Terms. The definition language could be taken from the April 26, 2019 ERO Enterprise CMEP Practice Guide on BES Cyber System Information: “An instance or event during which a user obtains and uses BCSI. For access to occur, in this context, a user, authorized or unauthorized, must concurrently both obtain BCSI and possess the ability to use BCSI. An unauthorized individual who obtains encrypted BCSI but has no ability to use it within a meaningful timeframe should not be considered to have access.”

Currently CIP-004-6 adequately addresses access controls to BCSI when stored by the responsible entity. The issue with the current access requirements is when applied to offsite vendors due to the fact that the Responsible Entity cannot control a vendor’s access to the BCSI.

With this definition in place the SDT can then simply change CIP-004-6 R4 to read:

R4: Process to authorize 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; and

4.1.3. BCSI Access

The SDT could also change language in CIP-004-6 R5.3 to read:

For termination actions, revoke the individual’s access to BES Cyber System Information, 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.

Part CIP-004-7 R4.1.3 would limit “BCSI Access” appropriately to vendors that are custodians to encrypted or otherwise masked data but do not have the ability to use it. Any vendor with both custody of data and ability to use it (e.g. have an encryption key) would need to be provisioned access by the Responsible Entity through their established access control process and procedures.

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 recommend that CIP-013 is expanded to include vendors that store BES CSI on behalf of entities. The vendor requirements in CIP-011 exceed CIP-013 requirements may result in additional processes that can be covered by the CIP-013 standard.

Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	No
Document Name	
Comment	

1. CIP-011 R1, Part 1.4 states "*Process(es) to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information*…." Since MEAG does not store its BCSI in the cloud with another vendor, would this requirement be **N/A**, or does MEAG still need to develop a risk assessment document (program/process) in the event we decide to use a cloud vendor for our BCSI in the future?

2. CIP-011 R2 deals with a key management program. Is this for physical and/or cyber? This requirement seems to assume that all entities would have a key server for authentication, revocation, etc. Is this only for those entities that are using a 3rd party vendor to store BCSI? However, what about those entities that don't issue 'keys'. For example, MEAG encrypts its files on the MEAG shared drive, but it is protected only by a secure password that is given to only a 3 people; the IS Administrators can't even see the contents of the files. Does MEAG need to call the software vendor to ask how files are encrypted by the software and how the keys get processed on the PC? The encryption on the files works in the background; MEAG has no control on that process. So, can this requirement be N/A for MEAG Power? Will N/A be allowed by the Auditors?

Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	

Duke Energy generally agrees that these requirements will promote a better understanding of security risks. Duke Energy would like better understanding of the opportunities to address appropriate security controls. Also, Duke Energy would like more clarity on what consitutues an acceptable risk assessment and/or what other options would suffice instead of a risk assessment.

Likes 0	
Dislikes 0	
Response	
William Hutchison - Southern Illinois Power Cooperative - 1	

Answer	No
Document Name	
Comment	
Comments: Doing a risk assessment of an 3rd party / offsite storage provider is practically useless. The best a RE will get from most providers is a SOC1 or SOC-2 report. The way this is written today only creates compliance risk and burden on the RE. The majority of offsite/Cloud provider storage solutions (a majority if not all the providers RE's would use) are not the issue when it comes to security risks. These types of businesses would not be in business if they did not have strong security systems in place and would not be used by Federal, State, Local governments and Fortune ranked companies. Instead of putting the burden on the RE, NERC/FERC needs create an approval process and keep an approved published list of 3rd party storage vendors list for RE's to be able to use. This is exactly what is done for government and government contractors. This would be more efficient, more in-depth, and not create compliance burden on the RE's. This would not restrict competition or violate any laws as any 3rd party would be able to go through the process to get approved.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	No
Document Name	
Comment	
This type of requirement often becomes a problem during enforcement, when the auditors evaluate the quality of the assessments. This is a reoccuring issue with the auditors, and can only be resolved through more specific wording in the requirements.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG is in agreement with RSC provided comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NextEra	
Answer	Yes
Document Name	

Comment
1) We have strong apprehensions on “mitigate” in Part 1.4 and possibly push some to vote NO on this project. See #2 for more feedback. 2) We agree with that Part 1.4 will promote a better understanding the security risks involved. We have serious concerns with these controls. Entities have little control of vendors OR the vendors of the primary vendors. We recommend the path laid out by CIP-013 – a) have a plan and b) implement that plan. The potential costs of these controls may not produce an effective result. Plus the submitted feedback to Standards Efficiency Review tends to question the value of annual reviews for the sake of a review instead of a trigger. 3) We request this SDT consider if these vendor controls (mitigations) belong in CIP-013. 4) No consensus on Part 2.1 5) We request clarification of physical security - will Part 2.2 be difficult to implement where the custodian and the person with the key are the same?

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	

Comment
Texas RE recommends the SDT define the term “vendor”, which is used in Part 1.4 as well as referenced in CIP-005-6 and CIP-013-1. This would ensure an understanding of what is considered a vendor.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	Yes
Document Name	

Comment
We believe the proposed vendor risk assessment is best under CIP-011 rather than combining with CIP-013.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	

Comment
IESO agrees in principle with the comments submitted by NPCC We agree with that Part 1.4 will promote a better understanding the security risks involved. We have serious concerns with these controls: 1. We have strong apprehensions on “mitigate” in Part 1.4 and possibly push some to vote NO on this project. Entities have little control of vendors their subcontractors vendors. We prefer the SDT consider that these vendor controls (mitigations) belong in CIP-013. If the SDT leaves these controls in CIP-011, we recommend the same type of strategy used in CIP-013 – a) have a plan and b) implement that plan rather that “mitigate” 2. In regards to Part 2.2 , we request clarification with respect to physical security - Part 2.2 may be difficult to implement where the custodian and the person with the key are the same?

Likes 0	
Dislikes 0	

Response

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

Comment
Please clarify if R1.4 would apply only to vendors providing storage as a service for BCSI, or if it would apply to any vendor possessing any amount of BCSI.

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

We would encourage the SDT to include a time frame for when 3rd party security mitigations need to be completed. It is an improvement to see that a date must be included for closure of identified security risks, but this is still open ended and will not ensure timely closure of risks.	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 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	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	

Answer	
Document Name	
Comment	
We support NPCC RSC comments.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	
Document Name	
Comment	
While this will promote a better understanding of the requirements, it suffers in that internally stored information does not require the same types of controls as externally stored information. For example, a company may encrypt all data storage, whether or not BCSI. However, requiring a separate key custody process for internally stored information in small registered entities is an excessive and overly prescriptive requirements.	
Likes 0	
Dislikes 0	
Response	

7. The SDT is addressing the growing demand for Responsible Entities to leverage new and future technologies such as cloud services. Do you agree that the proposed changes support this endeavor?

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	No
Document Name	

Comment

There is not enough detail to address large service providers who will not cooperate with an entity for risk assessments for cloud computing. Companies such as MicroSoft have not be very cooperative in helping us assure that the information is protected. All companies should be able to be held to a common 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 revisions make the use of specific technologies less apparent and adds to complexity. If cloud is permitted, it should list this as an example.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

As indicated in our previous responses, especially to Q3 and Q6, we believe that the proposed Requirements, by overly focusing on and prescribing technologies, will instead significantly increase administrative activities and costs as well as introduce significant new compliance risks, and may discouraging Responsible Entities from pursuing such options.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy support the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Jeremy Voll - Basin Electric Power Cooperative - 3

Answer	No
Document Name	

Comment

Support the MRO NSRF comments

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	

Comment

Agree with SDT's idea and disagree with the written language that is vague. Cloud storage and encryption technologies are not explicitly excluded under the current standards, where the registered entity could include NDA or contract provisions that require vendors to provide BCSI access and handling evidence in order to meet CIP-011 and CIP-004 requirements. Even though the new requirements R1.4 and R2 try to provide other cloud services solutions, we haven't see the cloud storage and encryption language in the revised requirements.

SDT should focus on revising or developing new requirements that meet the objective of protecting access to BCSI without constraining or prescribing types of storage solutions such as physical and electronic access controls. Any new Requirements need to address cloud services should clearly state that in the requirement language.

Currently CIP-004-6 adequately addresses access controls to BCSI when stored by the responsible entity. The issue with the current access requirements is when applied to offsite vendors due to the fact that the Responsible Entity cannot control a vendor's access to the BCSI even though NDA could be used for the compliance.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

Seattle supports the comments of SMUD to this question.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The changes do show support and leverage towards new and future technologies but they are too specific and do not provide flexibility for the various solutions and security controls that could vary.

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 focus needs to be on protecting access to the information. This should be performed in a vendor/platform neutral manner - whether the systems are administered by in-house personnel or hosted on a shared cloud-based hosting provider, the outcome, regardless, should be that access to the information is limited to authorized individuals only. As such, suggest re-architect the standard to be outcome based so as not to preclude using specific technologies or adoption of emergent solutions.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI supports comments filed by NRECA	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
NRECA agrees that the proposed revisions support this endeavor as related to specifically configured cloud storage services; however, we observe that the proposed revisions are very limiting relative to compatibility with future or differently configured storage solutions and impose new, different, and unnecessary compliance obligations on entities regardless of whether they are pursuing such options. NRECA is concerned that the way this has been	

incorporated outweighs the value of the proposed revisions relative to taking small steps toward addressing the use of could services. NRECA does not support the proposed revisions.	
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	
We agree with MRO NSRF comments: “we believe that the proposed Requirements, by overly focusing on and prescribing technologies, will instead significantly increase administrative activities and costs as well as introduce significant new compliance risks”.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
GSOC agrees that the proposed revisions support this endeavor as related to specifically configured cloud storage services; however, observes that the proposed revisions are very limiting relative to compatibility with future or differently configured storage solutions and impose new, different, and unnecessary compliance obligations on entities regardless of whether they are pursuing such options. For this reason, GSOC is concerned that the manner in which this has been incorporated outweighs the value of the proposed revisions relative to taking small steps toward addressing the use of cloud services. As well, GSOC notes, again, that standard revisions to accommodate cloud storage are unnecessary and would be better addressed in implementation or compliance guidance. For these reasons, GSOC does not support the proposed revisions.	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No

Document Name	
Comment	
SMEC agrees with comments submitted by NRECA.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
No because of Part 1.5 still requires revocation of individual access privileges for third party vendors. This requires additional administrative burden for entities as they have little control over third parties. As a suggestion, the SDT could consider wording vendor access controls within “have/ implement a plan which addresses risks associated with vendor access to BCSI”	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Understand the growing use of cloud services for storage solutions, but it may be simpler to have a stand alone standard that address just cloud storage or have the applicability for just cloud services.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No

Document Name	
Comment	

The requirements should be moved to appropriate standards. The vendor requirements should be moved to CIP-013 as applicable. Part of the SCRM plan should be evaluating cloud services to meet the needs of applicable standards in scope.

R1.4 - The proposed language describes actiosn which should occur in supply chain management and should not be addressed in CIP-011.

R1.4.3 – remove the term "Mitigation Plan." This is a confusing term which connotates a regulatory mitigation plan filed w/ the ERO.

R1.4.3 – "Remediate" and "mitigate" are different actions. Please choose one or the other when using these terms

Likes 0	
Dislikes 0	
Response	

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	
Comment	

I believe the team should consider specifying the security objectives for use of third-party storage solutions, and not limit the discussion to a risk profile similar to CIP-013. Understanding the third-party risk profile does not go far enough. When the third-party has access to an entity's BCSI, there must be a thorough understand of how the entity revents unauthorized access, manages and limits user permissions, etc. against a well-defined set of objectives.

Likes 0	
Dislikes 0	
Response	

Vivian Moser - APS - Arizona Public Service Co. - 3

Answer	No
Document Name	
Comment	

While the proposed requirements are a step in the right direction relative to cloud storage solutions, the language as written for Part 1.2 creates the unintended consequence of limiting the types of technology (current and future) that can be used due to the access management methods that would be necessary to implement and evidence. In support of AZPS's response to Question No. 4, AZPS believes leveraging new and future technologies would require a focus on preventing unauthorized access to identified storage locations as stated in Part 1.1, rather than a requirement to evidence

eliminating the ability to obtain and use. Alternatively, establishing a clear delineation between preventing unauthorized access to identified storage locations and the protection of BCSI during transit, use, and disposal would also provide ability to leverage different technologies.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
New and emerging technologies shift the paradigm of security controls away from a specific storage location/repository to the ability to access and use the information itself. For example, an entity that utilizes file level security can apply encrypted protections on the data that preclude unauthorized access to the data regardless of where it is stored. Requiring a list of storage locations is an antiquated construct that disincentivizes entities from using potentially more secure mechanisms because of the impossibility of compliance with documenting storage locations. The requirement should be technology agnostic and objective based, so it is written to focus on the implementation of effective methods that afford adequate security protections to prevent unauthorized access to the information.	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3	
Answer	No
Document Name	
Comment	
The changes do show support and leverage towards new and future technologies but they are too specific and do not provide flexibility for the various solutions and security controls that could vary.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	No

Document Name	
Comment	
See NRECA submitted comments.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes proposed requirements CIP-011-3 Requirement R1, Part 1.4, and R2 Parts 2.1 and 2.2 are more likely to inhibit the use of cloud-based BCSI storage solutions than to promote it.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We agree that the proposed changes address the demand to leverage new and future technologies. We disagee with the changes made to CIP-011 R1.3 and R1.5. This change expands the scope of these requirements beyond the original BCSI access requirements in CIP-004-6 R4 and R5 . We suggest that CIP-011 R1.3 and R1.5 be changed to processes related to designated BCSI storage locations, thus maintaining the spirit of the CIP-004 access management requirements.	
Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments. The current approach taken by the SDT appears too proscriptive and should remain flexiable and technology agnostic rather than stipulating a particular process or tool, such as key management.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC	
Answer	No
Document Name	
Comment	
NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES	
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	
This is very similar to Question 3. Please refer to Question 3 response.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
Yes, the proposed chages support future technologies but do not provide flexibility in as need.	
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	
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 response found in the NSRF Comment Form	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
Although the SDT is addressing the industry's request to add cloud services to store BSCI, the SDT needs to address the how to mitiage the individual terminations at third parties. It is unclear if the entities need to have an information agreement with individuals at a cloud service or with the cloud service company.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We agree that the proposed changes address the demand to leverage new and future technologies. *We disagee with the changes made to CIP-011 R1.3 and R1.5. This change expands the scope of these requirements beyond the original BCSI access requirements in CIP-004-6 R4 and R5 . We suggest that CIP-011 R1.3 and R1.5 be changed to processes related to designated BCSI storage locations, thus maintaining the spirit of the CIP-004 access management requirements.*	
Likes 0	
Dislikes 0	
Response	

Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	
No because of individual terminations at third parties.	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
We appreciate the SDT's efforts to make changes that allow entities to leverage new and future technologies. We believe that the changes made here do support the concept of using cloud services; however, those changes should not impact an entity that does not use that technology. The SDT should consider that not all entities will use cloud services and should ensure that the changes do not negatively impact or create an additional burden to those entities.	
Likes 0	
Dislikes 0	
Response	

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support MRO comments.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
The standards development team should support specific requirements providing appropriate levels of security for Cloud Service Providers and 3rd Party Access. Transferring the CIP-004 BCSI requirements to CIP-011 does not address the unique issues created by storing BCSI in repositories that are not controlled by registered entities. The standards development team should draft separate requirements.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
No. As written, the proposed changes may not sufficiently support this endeavor much more than the existing standards. MISO proposes the following changes to provide additional clarity. As noted under our response to question 1, to more clearly articulate the key distinctions mentioned during the Q&A portion of the 2019-02: BES Cyber System Information Access Management webinar hosted on January 16, 2020, MISO proposes the SDT expand the language of the last example provided under requirement R1, Part 1.1, Measures as follows:	

"Storage locations *(physical or electronic, responsible entity or vendor hosted)* identified for housing BES Cyber System Information in the entity's information protection program"	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI member companies appreciate the efforts by the SDT to enhance Responsible Entities ability to leverage new and future technologies such as cloud-based services. However, the framework, as written, is too narrow and could potentially limit the use of future innovations and technologies that might yield better security and efficiencies.	
Likes 0	
Dislikes 0	
Response	
Gregory Campoli - New York Independent System Operator - 2	
Answer	No
Document Name	
Comment	
NYISO feels that the proposed changes may not sufficiently support this endeavor more so than the language contained within the existing standards, NYISO offers the following suggested changes to provide additional clarity. NYISO proposes the SDT expand the language of the last example provided under requirement R1, Part 1.1, Measures as follows: "Storage locations of either physical or electronic data housed within a responsible entity's Physical Security Perimeter or housed within a vendor's hosted environment be identified as BES Cyber System Information locations as part of the entity's information protection program" NYISO understands that R1.4 and R2 attempts to cover this detail, however NYIOS feels that additional clarification is needed. NYISO's stance is that third party personnel may have physical or electronic access to encrypted BCSI, but as long as they do not have access to the keys for decrypting the BCSI, the information should be considered sufficiently protected.	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NextEra	
Answer	No
Document Name	
Comment	
No because of individual terminations at third parties.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
In our very the existing standard already allows. It appears NERC and FERC is not will to advertise this to entities.	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
Please see response to Question 3, above. Without explicit and affirmative language, the proposed change does nothing to clarify the issue. Entities will not likely move toward cloud storage for BCSI unless CIP language specifically supports cloud storage in those terms.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	

Answer	No
Document Name	
Comment	

Alliant Energy agrees with NSRF and EEI’s comments.

While Alliant Energy appreciates the SDT’s efforts to expand information storage solutions or security technologies for responsible entities, that expansion is only useful if the requirement language is written such that it is clearly auditable. The updated requirements should avoid the ability to audit to prescriptive requirements that are not stated in the language of the requirements.

Likes 0	
Dislikes 0	
Response	

Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3

Answer	No
Document Name	
Comment	

See Steven Toosevich's comments.

Likes 0	
Dislikes 0	
Response	

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	
Comment	

OPG is in agreement with RSC provided comment

Likes 0	
Dislikes 0	
Response	

James Brown - California ISO - 2 - WECC

Answer	No
Document Name	
Comment	
Please see comments to question #3 and #6.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE agrees with EEI's comments	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	No
Document Name	
Comment	
There is a significant barrier in the proposed language to adoption of cloud services with regard to the EACMS definition remaining as it stands. The proposed changes do not offer entities the opportunity to make use of Managed Security Service Providers (MPPS) for their most critical systems because the systems deployed by the MSSP would still fall into the EACMS bucket. A possible solution would be to move forward with a split of the EACMS definition into EACS and EAMS, with BCSI requirements (CIP-011) applying to EAMS, and system hardening requirements (CIP-006, CIP-007, & CIP-010) applying to EACS.	
Likes 0	
Dislikes 0	
Response	

Angela Gaines - Portland General Electric Co. - 1	
Answer	No
Document Name	
Comment	
Please see comments PGE Group 2	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
In our view the existing standard already allows. It appears NERC and FERC is not willing to advertise this to entities.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
We agree that the proposed changes address the demand to leverage new and future technologies. We disagee with the changes made to CIP-011 R1.3 and R1.5. This change expands the scope of these requirements beyond the original BCSI access requirements in CIP-004-6 R4 and R5. We suggest that CIP-011 R1.3 and R1.5 be changed to processes related to designated BCSI storage locations, thus maintaining the spirit of the CIP-004 access management requirements.	
Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT refers the drafting team to ERCOT's responses to Question Nos. 3 & 6.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
We agree that the proposed changes address the demand to leverage new and future technologies.	

We disagee with the changes made to CIP-011 R1.3 and R1.5. This change expands the scope of these requirements beyond the original BCSI access requirements in CIP-004-6 R4 and R5. We suggest that CIP-011 R1.3 and R1.5 be changed to processes related to designated BCSI storage locations, thus maintaining the spirit of the CIP-004 access management requirements.	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
Comments: No, see comments to question 6.	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
Agree with Tennessee Valley Authority's comments about protecting access in a vendor/platform neutral manner. The focus should not be on where it is stored but how access to the documents is secured.	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
The standard introduces appropriate controls for cloud storage environments. However, the standard is not specific to cloud storage and some of the items are not reasonable for internally stored information.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees that the SDT is addressing the growing demand for Responsible Entities to leverage new and future technologies such as cloud services. Duke Energy suggests that the SDT clarify the wording of the requirements to match those of the technical rationale document. Also, the requirements as written are problematic for reasons provided in previous and subsequent responses.	
Likes 0	

Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	Yes
Document Name	
Comment	
It is a good step forward. We need to have clarifying language for concerns previously identified.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA supports the SDT's direction; however, the language is not yet clear enough to adopt.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, 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 modifications clearly indicate that third-party providers of BCSI storage will be allowed and the objectives an entity should reach in determining the risks of the third-party usage and remediation or mitigation of those risks as determined by the entity. The non-prescriptive nature of some of the Requirement language such as "Method(s) to prevent unauthorized access" in CIP-011-3, R1, Part 1.2 could be unsettling to some entities who want to be told what needs to be done, but the objective nature provides the flexibility the SDT is trying to achieve to future proof the Standard as much as possible and not disallow technology or processes unknown to the SDT that a more prescriptive Requirement could disallow.	

As noted in Question 6, PG&E does have concerns regarding the overlap of CIP-011 R1 P1.4 with CIP-013 R1 P1.1.	
Likes 0	
Dislikes 0	
Response	
Colleen Campbell - AES - Indianapolis Power and Light Co. - 3	
Answer	Yes
Document Name	
Comment	
The requirement is a good start towards the security methodologies needed for cloud storage.	
Likes 0	
Dislikes 0	
Response	
William Hutchison - Southern Illinois Power Cooperative - 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	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
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	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kent Feliks - AEP - 3	
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	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	
Document Name	
Comment	
We are looking forward to improved wordings before answering this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	

Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	

8. The SDT is proposing a new "key management" set of requirements. Do you agree that key management involving BCSI is integral to protecting BCSI?

Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	

The requirement is unclear if this is an electronic key or a physical key. This will add considerable costs to smaller entities. This is an undue burden for the industry. If you control access through an effective DMS, behind firewalls, or through the cloud processes, adding electronic key controls as prescribed by the Standard is unnecessarily burdensome for entities.

Likes 0	
Dislikes 0	
Response	

Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	

Comments: No, see comments to question 6. In addition, the key management items should be listed in the measures. Encryption should not be the only acceptable method of protecting BCSI; methods should be based on risk. Recommendation: replace "key management" with "electronic data protection methodology."

Likes 0	
Dislikes 0	
Response	

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

R2 Applicability should be:

BES Cyber System Information stored in Vendor managed electronic BCSI Repositories, and pertaining to:

High Impact BES Cyber Systems and their associated:

1. EACMS; and

2. PACS; and

3. PCA

Medium Impact BES Cyber Systems with ERC and their associated:

1. EACMS; and

2. PACS; and

3. PCA

We recommend removing R2 from this Standard. Key management should not be specified as a means, as there are others. An entity should have the flexibility to use something from their key management program as evidence of a control, without mandating specific requirements in the standard. The ERO Enterprise CMEP Practice Guide: BES Cyber System Information dated April 26, 2019 suggests auditors review whether key management practices were implemented based on best practices. The SAR did not seek to increase required controls. Rather, it seeks language clarification around access controls and storage locations.

If R2 needs to be pursued, we recommend explicitly stating in R2.1 “develop cryptographic key process(es).” Add the term “cryptographic” as applicable within the R2 parts. Without the specificity, the Requirement could be interpreted to include both cryptographic, electronic and physical key management. We believe this was not the SDT’s intent.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

ERCOT does not believe there is a benefit to defining separate "key management" requirements. ERCOT proposes the removal of the explicit requirement and, if it is to be included at all, it should be included in the cloud vendor risk assessments considerations of Part 1.4 .

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

R2 Applicability should be:

BES Cyber System Information stored in Vendor managed electronic BCSI Repositories, and pertaining to:

High Impact BES Cyber Systems and their associated:

1. EACMS; and

2. PACS; and

3. PCA

Medium Impact BES Cyber Systems with ERC and their associated:

1. EACMS; and

2. PACS; and

3. PCA

We recommend removing R2 from this Standard. Key management should not be specified as a means, as there are others. An entity should have the flexibility to use something from their key management program as evidence of a control, without mandating specific requirements in the standard. The ERO Enterprise CMEP Practice Guide: BES Cyber System Information dated April 26, 2019 suggests auditors review whether key management practices were implemented based on best practices. The SAR did not seek to increase required controls. Rather, it seeks language clarification around access controls and storage locations.

If R2 needs to be pursued, we recommend explicitly stating in R2.1 “develop cryptographic key process(es).” Add the term “cryptographic” as applicable within the R2 parts. Without the specificity, the Requirement could be interpreted to include both cryptographic, electronic and physical key management. We believe this was not the SDT’s intent.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

The proposed version is prescriptive overkill.

Likes 0	
Dislikes 0	

Response

Angela Gaines - Portland General Electric Co. - 1

Answer	No
Document Name	

Comment

Please see comments PGE Group 2

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	No
Document Name	
Comment	
When used in the cloud, this is integral to encrypting that data, however the use of key management by itself does nothing to protect data. Additionally, when protecting BCSI on premise, there are many alternate controls that offer significant protections without the need to use key management infrastructure.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE agrees with EEI's comments	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
There is no benefit of defining separate key management requirements. Propose to remove the explicit requirement and, if at all, include in cloud vendor risk assessments considerations of R1.4.	
Likes 0	
Dislikes 0	
Response	

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG is in agreement with RSC provided comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	No
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI’s comments. Specifically, if key management is not a requirement (due to the “where applicable” language in 2.1), then it is not appropriate to have this language in the requirements section and would be better suited to guidance. The requirements should only state what is required. Additionally, it is unnecessary to require a key management program for all BCSI, which includes BCSI stored at responsible entity facilities and physical key management.	
Likes 0	
Dislikes 0	
Response	

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
A full and proper key management program/system is a big ask for small to medium utilities who could most benefit from cloud storage and/or managed third-party storage solutions. In this case, SNPD once again suggests, that CIP language specifically authorize a Federal IT certification as sufficient to account for proper and secure key management on the part of the certified vendor. For example, many other federal agencies use large MSSPs (Azure/AWS) to store and secure highly sensitive information without the requirement to locally control the keys. If this is sufficient for large federal agencies involved in national security, it seems that the same could be applied to BCSI. If local key management is maintained as a requirement within the proposed changes, SNPD believes many utilities will take the path of least resistance, and/or the most conservative response and simply choose to avoid cloud storage altogether – depriving utilities most in need of flexible off-prem storage the ability to realize the benefits.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
The proposed version is prescriptive overkill	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro requests that additional clarity on the definition and application of "keys" as it relates to BCSI storage locations is provided before a determination if this is integral to protecting BCSI can be made. During the NERC webinar on the proposed revisions it was indicated that keys are inclusive of encryption passwords that enable an individual to access encrypted BCSI as well as physical keys that are used to access physical BCSI storage locations; however, this is not considered sufficiently clear per the standard language.	

Likes 1	BC Hydro and Power Authority, 5, Hamilton Harding Helen
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NextEra

Answer	No
Document Name	

Comment

1) We recommend “electronic data protection methodology” instead of “key management”.

2) We recommend moving the “key management” language to the Measures.

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2

Answer	No
Document Name	

Comment

NYISO feels that the requirements are too prescriptive regarding key management processes, administratively burdensome and lack a commensurate tie to what is the measurable expected outcome; i.e. a) a stated level of reliability performance, b) a reduction in a specified reliability risk (prevention), or c) a necessary competency. As noted under our response to question #6, NYISO recommends proposed CIP-011-3, requirement R2, Parts 2.1 and 2.2 be eliminated altogether and that key management be incorporated as an example under requirement R1.

NYISO would like to see terms such as cryptographic system or cryptosystem used. If the intent is that physical keys / locks are also a part of this mandate, it should be stated explicitly. In general, encryption should not be the only acceptable method of protecting BCSI. The selected methods should be based on risk.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment
EEI supports the use of “key management” for protecting BCSI at third party facilities. However, BCSI stored at responsible entity facilities are addressed in CIP-004-6 and CIP-011-2 Reliability Standards and therefore should remain an effective compliance solution with only minor modifications. The SDT should define the reliability objectives, not the method that must be used to accomplish the objective so that future technologies that might provide better protections can be used.

Likes 0	
Dislikes 0	

Response

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

Comment
The requirements fail to state specifically when a key management program is required. The requirement in Part 2.1 starts off with, “Where applicable“, but there is no information in the proposed CIP-011-3 that provides any information on where or when it is applicable. The Technical Rationale also fails to provide any clarity on where or when a key program is needed. Also the use of term “key” by itself causes confusion on whether the requirement is referring to encryption keys or physical keys for mechanical locks. If the SDT is referring to encryption keys then they should use the term “encryption key”.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	

Comment
No – as written the requirements are too prescriptive to key management processes, administratively burdensome and lack a commensurate tie to what is the measurable expected outcome; i.e. a) a stated level of reliability performance, b) a reduction in a specified reliability risk (prevention), or c) a necessary competency. As noted under our response to question 6, MISO recommends proposed CIP-011-3, requirement R2, Parts 2.1 and 2.2 be eliminated altogether and that key management be incorporated as an example under requirement R1.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
The standards development team should state explicitly that "Key Management" refers to encryption keys.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support MRO comments.	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
We agree that in today's environment, key management is widely used to support and manage the protection of information. However, our concern is that when the technology advances, these changes become "outdated" and put the industry in the same spot we are today. Whenever the opportunity arises to make changes to the standards, those changes should be risk-based and should not include a single technology solution.	
Likes 0	
Dislikes 0	
Response	

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

We recommend “electronic data protection methodology” instead of “key management”.

We recommend moving the “key management” language to the Measures.

If Key Management must be included, it should be ‘specific’, including the allowable key management options (rather than a long, and somewhat ‘vague’ list of possible controls).

Likes 0	
Dislikes 0	
Response	

Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	
Response	

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

R2 Applicability should be:

BES Cyber System Information stored in Vendor managed electronic BCSI Repositories, and pertaining to:

High Impact BES Cyber Systems and their associated:

1. EACMS; and

2. PACS; and

3. PCA

Medium Impact BES Cyber Systems with ERC and their associated:

1. EACMS; and

2. PACS; and

3. PCA

We recommend removing R2 from this Standard, key management should not be specified as a means, as there are others. An entity should have the flexibility to use something from their key management program as evidence of a control, without mandating specific requirements in the standard. The ERO Enterprise CMEP Practice Guide: BES Cyber System Information dated April 26, 2019 suggests auditors review whether key management practices were implement based on best practices. The SAR did not seek to increase required controls. Rather, it seeks language clarification around access controls and storage locations.

If R2 needs to be pursued, we recommend explicitly stating in R2.1 "develop cryptographic key process(es)." Add the term "cryptographic" as applicable within the R2 parts. Without the specificity, the Requirement could be interpreted to include both cryptographic, electronic and physical key management. We believe this was not the SDT's intent.

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 response found in the NSRF Comment Form

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. Additionally, SDG&E believes there is much ambiguity in the section describing the "key management program." There should be more clarity on whether these are physical keys or software keys. The goal of this key management program needs to be clearly defined. SDG&E also seeks clarification on what items qualify to be in scope for the key management program. For example, SDG&E's Information Protection procedure accounts for unattended BCSI in transit (*e.g.*, locked vehicle, locked briefcase, etc.). Since the SDT's proposed changes are more focused on BCSI rather than the storage location, this set of proposed requirements could bring in previously undesignated/unidentified locations into scope, such as locked vehicles and locked briefcases.

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 key management is integral to protecting unencrypted BCSI. We do agree that key management of encrypted material is integral to protecting any encrypted information. This question *assumes* all BCSI is encrypted and that **is not** the case. However, we believe the detailed prescriptive requirements in R2 may work against the goal of being able to use cloud services. For example, 8 different areas must be included in the key management program which are not discussed in the Technical Rationale document. A Google search of "Key suppression" shows no results applicable to this requirement so entities are left to guess what is meant by the words chosen in the requirement. Southern also questions why key revocation is listed twice in the same requirement part. Southern recommends that the areas of key management required are further defined and included in the Technical Rationale. Furthermore, Southern recommends that future proposed revisions of the Standard maintain the flexibility of **not requiring** encryption of BCSI when other controls can be implemented, such as access control solutions. Key management practices should be based on best practices and would be reviewed and measured as such during audit review. For Part 2.2, new terms and concepts are introduced that have no explanation, such as "BCSI Custodial entity" and their "custodial entity duties". Southern believes this requirement part is unnecessary as R1 is all about ensuring only authorized access is allowed to BCSI. Those who manage the encryption keys are required to have access to perform such management, so a non-compliance issue with 2.2 is really a non-compliance issue with R1 and Southern believes that only R1 is required to cover this risk.

Likes 0	
Dislikes 0	

Response

Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC	
Answer	No
Document Name	
Comment	
NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments. The current approach taken by the SDT appears too proscriptive and should remain flexiable and technology agnostic rather than stipulating a particular process or tool, such as key management.	
Likes 0	
Dislikes 0	
Response	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes cryptographic key management is necessary for electronic information but the language proposed so far causes problems for physical information storage (i.e., printed documents.)	
Likes 0	
Dislikes 0	
Response	

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

R2 Applicability should be:

BES Cyber System Information stored in Vendor managed electronic BCSI Repositories, and pertaining to:

High Impact BES Cyber Systems and their associated:

1. EACMS; and

2. PACS; and

3. PCA

Medium Impact BES Cyber Systems with ERC and their associated:

1. EACMS; and

2. PACS; and

3. PCA

We recommend removing R2 from this Standard, key management should not be specified as a means, as there are others. An entity should have the flexibility to use something from their key management program as evidence of a control, without mandating specific requirements in the standard. The ERO Enterprise CMEP Practice Guide: BES Cyber System Information dated April 26, 2019 suggests auditors review whether key management practices were implement based on best practices. The SAR did not seek to increase required controls. Rather, it seeks language clarification around access controls and storage locations.

If R2 needs to be pursued, we recommend explicitly stating in R2.1 “develop cryptographic key process(es).” Add the term “cryptographic” as applicable within the R2 parts. Without the specificity, the Requirement could be interpreted to include both cryptographic, electronic and physical key management. We believe this was not the SDT’s intent.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST considers proposed Requirement R2, Parts 2.1 and 2.2 vastly over-prescriptive. The goal here is to ensure that no individuals who manage BCSI storage, whether in the Responsible Entity’s own data center or “in the cloud,” can access BCSI unless they have been properly authorized in accordance with the requirements of CIP-004. Encryption and key management are certainly viable options, but they should remain options. N&ST suggests moving them to the “Measures” associated with an appropriately re-worded requirement.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

See NRECA submitted comments.

Likes 0	
Dislikes 0	

Response
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3
Answer	No
Document Name	
Comment
Managing keys does play an important role for protecting BCSI but in order to fully utilize new technology, key management cannot be the sole focus. It is important to ensure there are other layered security measures in place to allow for flexibility with keys. Not all new and future technologies can be implemented with such restricted key management requirements. Instead, we recommend the requirements be converted to objective-based requirements by removing “which shall include the following: 2.1.1-2.1.9.”
Likes 0	
Dislikes 0	
Response
Vivian Moser - APS - Arizona Public Service Co. - 3
Answer	No
Document Name	
Comment
AZPS does not agree that the proposed requirement to implement a key management program is integral to protecting BCSI. The addition of a requirement for a specific access control method (i.e., a key management program) is too prescriptive. AZPS recommends the same approach as discussed in previous comments above, wherein the focus remains on the protection of BCSI, rather than requiring specific controls. AZPS believes that Entities are well-positioned to assess and implement access control methods best suited to protect their BCSI. The Technical Rationale for CIP-011-3 states that a key management program provides an extra “layer of defense against bad actors who may have the means to physically or electronically obtain BCSI but not use or modify BCSI but not use or modify BCSI”. AZPS does not believe that the risk associated with obtaining BCSI but not being able to use or modify BCSI does not support implementation of a key management program.
Likes 0	
Dislikes 0	
Response
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5
Answer	No
Document Name	
Comment

No. Please see response to Q6. Key management is a possible measure for preventing unauthorized access, not an independent requirement.

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Key management should be a requirement for off-site storage of BCSI or BCSI in the cloud.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

We recommend “electronic data protection methodology” instead of “key management” which is too prescriptive
We recommend moving the “key management” language to the Measures
We would prefer the “If Applicable” to include language that says this is mandatory only if you are using encryption or encrypted protocols

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	No
Document Name	

Comment

SMEC agrees with comments submitted by NRECA.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

If selected as the security control to for access to BCSI, then, encryption is integral to protecting BCSI. However, encryption is not the only method or security control to the overall protection of BCSI. The focus of the “key management” requirements that were added to CIP-011, while helpful where encryption is utilized, are somewhat limiting to and leave unaddressed other methods and security controls that could be employed to protect BCSI. Further, use of the term “key” could create confusion and ambiguity regarding the scope of these requirements, e.g., does it address electronic and physical key management or merely electronic key management. Finally, GSOC is concerned that, as written, these new requirements may not be flexible enough to maintain applicability #3 technology changes and evolves. Please refer to GSOC’s response to question for additional comments regarding the limited applicability of these newly proposed requirements.

Additionally, GSOC notes that “custodial entity” is an undefined term and, therefore, could be interpreted broadly and variably. Further, there is not a clear indication of where or how the “controls” would be documented and maintained. This is significant as it interpretations of how to demonstrate compliance during compliance monitoring could vary across entities during implementation and across regions and audit teams, resulting in inconsistency in enforcement. As well, the use of the term “methods” within the measures has the potential to further complicate implementation and interpretation.

Finally, GSOC is concerned that a single control failure would result in a violation of requirement R2.2 regardless of whether other controls existed and duties remained separated. GSOC respectfully asserts that such ambiguity places auditors and Responsible Entities in uncertain and tenuous positions that would likely cause both to militate toward conservatism, resulting in over-reporting and -enforcement. For these reasons, GSOC requests that the SDT provide clarification of the term “custodial entity,” the expected compliance documentation, and the overall compliance obligation to avoid unnecessary compliance activities and risk.

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

R2 Parts 2.1 and 2.2 exceed the scope of the SAR and significantly increase the compliance obligations. CIP-011 should remain non-prescriptive and allow entities to implement the controls appropriate to their situations, which could be something other than encryption and key management. An entity is free to use something from their key management program if they have one to use as evidence of a control, without mandating specific requirements

in the standard. The ERO Enterprise CMEP Practice Guide: BES Cyber System Information dated April 26, 2019 suggests auditors review whether key management practices were implement based on best practices.

It is also unclear as to what “where applicable” means, and whether this requirement applies to physical keys and passwords to on premises systems.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

If selected as the security control for access to BCSI, then, encryption is integral to protecting BCSI. However, encryption is not the only method or security control to the overall protection of BCSI. The focus of the “key management” requirements that were added to CIP-011, while helpful where encryption is utilized, are somewhat limiting to and leave unaddressed other methods and security controls that could be employed to protect BCSI. Further, use of the term “key” could create confusion and ambiguity regarding the scope of these requirements, e.g., does it address electronic and physical key management or merely electronic key management.

Additionally, NRECA notes that “custodial entity” is an undefined term and, therefore, could be interpreted broadly and variably. Further, there is not a clear indication of where or how the “controls” would be documented and maintained. This is significant as interpretations of how to demonstrate compliance during compliance monitoring could vary across entities during implementation and across regions and audit teams, resulting in inconsistent enforcement. As well, the use of the term “methods” within the measures has the potential to further complicate implementation and interpretation.

Finally, NRECA is concerned that a single control failure would result in a violation of requirement R2.2 regardless of whether other controls existed, and duties remained separated. NRECA believes such ambiguity places auditors and Responsible Entities in uncertain and tenuous positions that would likely result in over-reporting and -enforcement. NRECA requests that the SDT provide clarification of the term “custodial entity,” the expected compliance documentation, and the overall compliance obligation to avoid unnecessary compliance activities and risk.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

AECI supports comments filed by NRECA

Likes 0	

Dislikes 0	
Response	
Kent Feliks - AEP - 3	
Answer	No
Document Name	
Comment	
AEP is of the opinion that key management methods can be either partially accessible or not accessible at all in certain cloud storage environments, which could increase security risks associated with the protection of BCSI. We also feel it is unnecessary to develop a key management process for the storage of BCSI within a Responsible Entity's own facility, but without more clarification surrounding the "where applicable" language, we are unsure if the language is specifically addressing third party storage locations or BCSI storage as a whole.	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
While Black Hills does agree that key management is crucial and appreciates it addition, we think further clarification should be added for information held by a provider or third-party. If the intent is for on-premis items as well, we think that key management should be listed as an example of possible controls and not the sole means.	
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	
As such, suggest re-architect the standard to be outcome based so as not to preclude using specific technologies or adoption of emergent solutions. As such, geo-location or biometric protections are not available as options to RE's.	

Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
We support NPCC RSC comments.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Managing keys does play an important role for protecting BCSI but in order to fully utilize new technology, key management cannot be the sole focus. It is important to ensure there are other layered security measures in place to allow for flexibility with keys. Not all new and future technologies can be implemented with such restricted key management requirements. Instead, Tri-State recommends the requirements be converted to objective-based requirements by removing “which shall include the following: 2.1.1-2.1.9.”	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
Although key management can be an effective control and a good security practice, it is not integral to protecting BCSI in all cases. Focusing attention on this one type of control once again ties the Standard to a specific technology concept that 1) is not applicable in all cases, 2) may become obsolete in part or in whole from unexpected technological developments, and 3) stifles alternative and creative approaches to security. Seattle believes key	

management should NOT be a specific requirement of the revised CIP-011, but it should be identified in the Measures and discussed in detail in the guidance documents as one effective approach that can be applied in many (but not all) situations.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
Agree with the proposing a new “key management” set of requirements, but need clarification for the written language in R2 (See our response in Question 6).	
Likes 0	
Dislikes 0	
Response	
Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy support the comments submitted by EEI.	

Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
Key management should not be specified as the means; Entities should be free to pursue any means that achieves the objective. We believe protecting BCSI is best handled in the CIP-004 Access Control Requirements. R2 Part 2.1 should be deleted in its entirety.	
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	
Including a key management requirement may burden entities who do not have a key managmenet infrastructure. The requirement also requires encryption as a technology that some entities may not want to employ.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	No
Document Name	
Comment	

We believe that this requirement is currently not adequately defined. The requirement language implies that this refers to encryption key management, but the technical rationale includes a physical component. It is not a trivial task to encrypt ALL BCSI, so please clarify that a key management program is not required for situations where BCSI is protected via another means. The technical guidance contains only two paragraphs for a key management program with nine management requirements. Please include technical examples that would suitable comply with each of the nine key management activities.

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller

Answer	No
Document Name	

Comment

This question is ambiguos and need more clarity. "key managment" ? Proposed language is not sufficient. Stating no here to insure other concerns are addressed.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Duke Energy does not agree with the new “key management” set of requirements. Duke Energy would like clarification if key management applies to electronic keys only and not physical keys. It is unclear what constitutes a custodial entity. It ignores other options for securing physical BCSI (e.g. badged access), and other forms of physical controls that could be used for access to physical BCSI.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 3

Answer	No

Document Name	
Comment	
The standard is appropriate for externally stored information under the direct control of the entity such as in a cloud environment. However, two cases where this is unreasonable: (1) Information stored by a consulting partner under non-disclosure agreement on systems owned and operated by a consulting partner. (2) Information stored internally on entity owned systems where the company has chosen to perform encryption for other reasons. I would not look forward to maintaining a key management program on each Microsoft Windows computer protected with BitDefender.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	No
Document Name	
Comment	
This represents a large burden on smaller utilities and those who outsource support.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, 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 agrees the addition of key management will be critical to the protection of BCSI not only in third-party environments, but also for internal usage to protect BCSI. Key management will demonstrate to Audit Teams the entity has the BCSI protected, and a lack of key management will raise serious concerns on how the BCSI is being protected. As noted in Question 6, PG&E recommends the requirement language clearly indicate key management covers the physical and electronic types of keys.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

While “key management” is one way to effectively protect BCSI, this is too prescriptive in dictating “how” to comply, and therefore not future proof. The requirement should be technology agnostic and objective based, so it is written to focus on the implementation of effective methods that afford adequate security protections to prevent unauthorized access to the information, so it is scalable and does not preclude use of new and emerging technologies as they become available.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	Yes
Document Name	

Comment

R2. - Encryption of BCSI and key management is the only potential method for entities to be able to utilize cloud services yet control CIA of data. It is imperative that access control include encryption as a method to prevent access

Likes 0	
Dislikes 0	

Response

Colleen Campbell - AES - Indianapolis Power and Light Co. - 3

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, 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	
Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
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	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
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	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
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	
William Hutchison - Southern Illinois Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
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	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	

9. The SDT is proposing to shift the focus of security of BCSI more towards the BCSI itself rather than physical security or "hardware" storage locations. Do you agree that this approach aids the Responsible Entity by reducing potential unneeded controls on BCS?

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

Answer	No
Document Name	

Comment

Duke Energy does not agree that to the significant change of focus to BCSI from BCSI designated storage locations, additional controls, compliance processes, and evidentiary documentation at a significant cost would be required along with requiring significant efforts of a technical, administrative, and operational nature to meet the new Requirements.

CIP-011-3, R1, Part 1.3 - "focus changed from access to designated storage locations to access to BES Cyber System Information" It is not clearly defined what information, independently or collectively, establishes the designation of BES CSI. The review and management of current designated storage locations (and data) are managed by designated employees. The requirement that all potential BES CSI is guarded in transit and use increases the number of individuals requiring training and potential access to the repository. An independent host name or IP address, independently, is not currently labeled BES CSI. An individual without NERC privileges may have that information for daily work at a Generation station.

CIP-011-3, R1, Part 1.6 - "focus of verification changed from designated storage locations to BES Cyber System Information: It is not clearly defined what information, independently or collectively, establishes the designation of BES CSI. An independent host name or IP address, independently, is not currently labeled BES CSI. It is not possible for a small subset of individuals to review and manage all data throughout generation stations that 'may be' considered BES CSI based on an unclear definition.

CIP-011-3, R1 Part 1.5 "focus of termination actions changed from access to designated storage location to access to BES Cyber System Information". This is not feasible in the case of individuals access to documentation that is considered "in use" such as hard copies of information. It is not feasible to manage at the document level while removing access from repositories can occur electronically and instantly.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

As written, this will have the opposite impact due to the focus on the lifecycle of BCSI. Any BCSI that is stored and transmitted by BCS, EACMS, PACS, or PCAs will now require specific protections. For example, BCSI stored in ourBCS will now need to have extra protections during storage and transit between BCS ad associated assets above what is required for operation for the BCS. This is not itself a bad thing, but as written this will be required by the proposed changes.

Likes 0	
Dislikes 0	

Response
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller
Answer	No
Document Name	
Comment
Needs further discussion and clarification.
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
Specifically focusing on storage locations defined what to protect. Entities may not know the location of BES CSI at all times when in use and transit.
Likes 0	
Dislikes 0	
Response
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF
Answer	No
Document Name	
Comment
The approach will significantly increase unnecessary controls on BCSI by eliminating the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems, and adding authorization/revocation and review requirements for all BCSI, instead of only on identified storage locations. If the intent is to shift the focus to the BCSI rather than storage locations, why is there a requirement to list storage locations (R1 Part 1.1)? See also comments to question 1. Not sure what is meant by unneeded controls on BCS.

As to the concept itself, we believe it will be more difficult to apply requirements to BCSI than the assets or storage locations in which it resides, and therefore are resistant to this approach. Better to define BCSI Repositories and BCSI Access per previous responses.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy support the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
Disgree with eliminating BCSI storage locations. If the intent is to shift the focus to the BCSI rather than storage locations, why is there a requirement to list storage locations (R1 Part 1.1)? We believe BCSI Repository identification (see our response in Question 1) is centric for preventing unauthorized	

access to the BCSI in that it is difficult to apply requirements to BCSI than the assets or storage locations in which it resides. For example, if a person wants to have an authorized access to BCSI, he (she) should request access to the BCSI respository first. This approach ensures the person who possess the BCSI will always has authorized access to the BCSI. The BCSI Repository and BCSI requirements should be working together to prevent unauthorized access to BCSI.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

Seattle is concerned that this proposed approach reopens the challenges of protecting individual “pieces” of BCSI that plagued CIP v1-3, adds complexity, and introduces unintended consequences. This change ultimately MIGHT be the most effective one, but it should be vetted and explored and explained in much more detail to minimize perverse outcomes.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Tri-State understands and agrees with the intent, however, as currently drafted, applicability and how to comply with the requirements become blurred. For example, if the requirements are kept focused on designated storage locations for BCSI, it eliminates confusion with BCSI that may reside in BCS, EACMS and PACS. We understand that this is a challenging part of the project, but we are concerned that the applicability and associated requirements as currently drafted will create confusion, redundancy and expanded scope. Other than reverting back to the original structure, a possible solution could be to add exclusions to the applicability to exclude High and Medium Impact BCS and their associated EACMS and PACS.

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	
This increases a entities controls that are needed for BCSI. An entity would have to defined multiple process elements to further define and control BCSI while it is in flight or in all storage locations that could have BCSI.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3	
Answer	No
Document Name	
Comment	
AEP does not agree that this approach reduces potential unneeded controls on BCS. Additional BCSI related requirements feel unnecessary, and we feel making modifications to access control requirements could address this issue.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI supports comments filed by NRECA	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	

Answer	No
Document Name	
Comment	
While this approach may reduce the potential for unnecessary controls on BCS, it introduces significant other compliance activities/obligations and required security controls with which Responsible Entities must comply. Accordingly, the revised approach does not achieve a net reduction in effort or scope of security controls and – likely – results in an increase of same without any resulting increase in security or reliability.	
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	
While we agree with the approach, the draft does not accomplish this. The focus can be shifted to the BCSI itself to meet the goals of the SAR by slightly modifying CIP-004 R4, Part 1.4.3 to [Process to authorize. . .] “Access to BES Cyber System Information in designated storage locations.” The focus of CIP-011 has always been on the BCSI, so we contend that the changes proposed in R3 directly contradict this by changing the focus to the assets and storage media, rather than the BCSI.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
While this approach may reduce the potential for unnecessary controls on BCS, it introduces significant other compliance activities/obligations and required security controls with which Responsible Entities must comply. Accordingly, the revised approach does not achieve a net reduction in effort or scope of security controls and – likely – results in an increase of same without any attendant increase in security or reliability.	
Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC agrees with comments submitted by NRECA.	
Likes 0	
Dislikes 0	
Response	

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
The proposed changes do not reduce potential uneeded controls on BCSI it adds more controls.	
Likes 0	
Dislikes 0	
Response	

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
I do not believe this will lessen the controls as security will still be needed for the physical locations as well. Further, the proposed standard provides greater specificity in R1 Part 1.1 in identifying BCSI storage locations.	
Likes 0	
Dislikes 0	
Response	

Vivian Moser - APS - Arizona Public Service Co. - 3	
Answer	No
Document Name	
Comment	
Although AZPS agrees that the proposed requirements reflect an intent to increase security controls to protect BCSI, protection through management of access to storage locations should remain separate from protection of BCSI in transit, use, and disposal.	
Likes 0	
Dislikes 0	
Response	

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3	
Answer	No
Document Name	
Comment	
Tri-State G&T understands and agrees with the intent, however, as currently drafted, applicability and how to comply with the requirements become blurred. For example, if the requirements are kept focused on designated storage locations for BCSI, it eliminates confusion with BCSI that may reside in BCS, EACMS and PACS. We understand that this is a challenging part of the project, but we are concerned that the applicability and associated requirements as currently drafted will create confusion, redundancy and expanded scope. Other than reverting back to the original structure, a possible solution could be to add exclusions to the applicability to exclude High and Medium Impact BCS and their associated EACMS and PACS.	
Likes 0	
Dislikes 0	
Response	

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
See NRECA submitted comments.	
Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

N&ST is curious to know what “potential unneeded controls on BCS” might be reduced by changing the existing requirement to manage access to BCSI storage locations to a requirement to grant, review, and revoke access to BCSI itself. In any case, N&ST believes such a change would have the potential to significantly increase a Responsible Entity’s access management program workload and significantly increase its compliance risk (how would an Entity convincingly demonstrate revocation of access to BCSI had been accomplished within the prescribed time frame?), with little or no reduction of risk to BES Cyber Systems and the BES. N&ST believes the existing requirements of CIP-011 implicitly but adequately convey an obligation to ensure BCSI cannot be accessed by unauthorized individuals.

N&ST strongly opposes this proposed change.

Likes 0	
Dislikes 0	
Response	

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

We are concerned with this approach. Authorizing access to BCSI is problematic unless the access requirements and controls are specific to the designated BCSI storage locations.

The approach will significantly increase controls on BCSI by eliminating the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems, and adding authorization/revocation and review requirements for all BCSI, instead of only on designated storage locations. As stated previously, there is no benefit to these additions because without ERC, a bad player would not be able to remotely access and use the information.

We believe that focusing on access controls to storage locations adequately address the risks. A shift of focus to the BCSI rather than storage locations is unnecessary and only ads significant burdens and impossible evidentiary requirements.

Likes 0	
Dislikes 0	
Response	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA finds the strategy is reasonable but implementation of the exact verbiage needs care. Various cyber security methodologies often address cyber system protection strategies and information protection strategies separately. It's also necessary to address the Cyber Asset definition where it includes "data in the device" to clarify and make the language consistent. Potential conflict between proposed requirements for protecting system data vs requirements protecting systems/devices would be very bad. The positive side of protecting the information rather than the storage location is that specific controls for digital information such as encryption come into scope and these methods are very effective when properly implemented. 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.	
Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments. Physical locations may require a different approach from cloud based storage of BCSI data.	
Likes 0	
Dislikes 0	
Response	

David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	

Dislikes 0	
Response	
Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC	
Answer	No
Document Name	
Comment	
NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES	
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 agrees that certain hardware/device/Cyber Asset level requirements (such as CIP-011 R2) must change in order to allow for cloud services. However, Southern does not agree that a wholesale move to protecting BCSI rather than BCSI storage locations is measurable or auditable as per our answer to Question 2. In essence, Southern agrees that the focus needs to change from BCSI physical or hardware storage locations. However, “BCSI storage location” does not necessarily imply physical or hardware issues, it can just as easily point to a dedicated and protected area within a cloud service offering. CIP-011-1’s current R2 needs to be updated so that it is **not** Cyber Asset and physical media based, however in this proposal it remains as such.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
See response in question #6 and #7.	

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. Additionally, for proposed CIP-011-3 R3.1, SDG&E suggests the draft retain the language "…that contain BES Cyber System information…" Otherwise there is a requirement to sanitize assets which may not contain BCSI and may not have an available method for sanitization.	
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 response found in the NSRF Comment Form	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We are concerned with this approach. Authorizing access to BCSI is problematic unless the access requirements and controls are specific to the designated BCSI storage locations.	

The approach will significantly increase controls on BCSI by eliminating the qualifying language "with ERC" from the applicability of Medium Impact BES Cyber Systems, and adding authorization/revocation and review requirements for all BCSI, instead of only on designated storage locations. As stated previously, there is no benefit to these additions because without ERC, a bad player would not be able to remotely access and use the information.

We believe that focusing on access controls to storage locations adequately address the risks. A shift of focus to the BCSI rather than storage locations is unnecessary and only ads significant burdens and impossible evidentiary requirements.

Likes 0	
Dislikes 0	

Response

Ayman Samaan - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

We agree with this approach but we believe this update is not backwards compatible (primarily because of the new Applicability / storage locations).

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	
Comment	
Support MRO comments.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
There is no opportunity in the proposed standards to reduce controls on BCS, rather the proposed changes represent a vast increase in required security controls and evidence gathering obligations.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI does not support additional Requirements to BCSI. Instead, the recommendations contained within our response to Question 4 could provide an equally effective solution resulting in fewer changes to existing processes for responsible entities. In addition, the inclusion of the undefined term of “storage locations” may create new obligations for entities who desire to use third party storage locations. This would necessitate that entities continue to identify and protect the physical location and hardware of host repositories. This may keep industry from using cloud-based services. As an alternative, the requirements could be written to only require entities to identify the repository name, type of repository (electronic or physical) and identifying if the repository is managed onsite by the responsible entity or offsite by a third party.	
Likes 0	
Dislikes 0	
Response	

Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
I would agree if that were the approach; and if this proposal was not so prescriptive; and if this proposal was not so way out to the SAR scope.	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
We agree with the approach however the language in the requirement does not achieve this goal. If the desire is to securely handle the information itself, SNPD suggests a mandatory labelling and protection scheme akin to DoD requirements for protection of classified data. Requirements are clear, implementation is simple, and accountability is baked in.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	

Answer	No
Document Name	
Comment	
The definition of storage locations needs to include references to physical protections. A shift away from physical protections or 'hardware' dilutes the concept of security around BCSI.	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
See comments for Part 1.1. Shifting the emphasis away from where the information is stored will increase potential unneeded controls for BCSI. Rather than focusing on the systematic protection of those locations where controls can be applied, the revisions can be seen as requiring protection of individual pieces of information. This would be tremendously burdensome and possibly unattainable.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE agrees with EEI's comments	
Likes 0	
Dislikes 0	
Response	
Angela Gaines - Portland General Electric Co. - 1	

Answer	No
Document Name	
Comment	
Please see comments PGE Group 2	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
I would agree if that were the approach; and if this proposal was not so prescriptive; and if it was not so way out of the SAR scope.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
We are concerned with this approach. Authorizing access to BCSI is problematic unless the access requirements and controls are specific to the designated BCSI storage locations. The approach will significantly increase controls on BCSI by eliminating the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems, and adding authorization/revocation and review requirements for all BCSI, instead of only on designated storage locations. As stated previously, there is no benefit to these additions because without ERC, a bad player would not be able to remotely access and use the information. We believe that focusing on access controls to storage locations adequately address the risks. A shift of focus to the BCSI rather than storage locations is unnecessary and only adds significant burdens and impossible evidentiary requirements.	
Likes 0	
Dislikes 0	

Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT refers to its comments concerning Part 1.1., and believes that shifting the emphasis away from where the information is stored will increase the potential of unneeded controls for BCSI. Rather than focusing on the systematic protection of those locations where controls can be applied, the revisions can be seen as requiring protection of individual pieces of information. Requiring protection of individual pieces of information would be tremendously burdensome and possibly unattainable.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

We are concerned with this approach. Authorizing access to BCSI is problematic unless the access requirements and controls are specific to the designated BCSI storage locations.

The approach will significantly increase controls on BCSI by eliminating the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems, and adding authorization/revocation and review requirements for all BCSI, instead of only on designated storage locations. As stated previously, there is no benefit to these additions because without ERC, a bad player would not be able to remotely access and use the information.

We believe that focusing on access controls to storage locations adequately address the risks. A shift of focus to the BCSI rather than storage locations is unnecessary and only adds significant burdens and impossible evidentiary requirements.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

It is agreed that the focus should be on protecting the BCSI and Responsible Entities should have the flexibility to build a program that best fits their needs. These revisions seem to focus mostly on encrypting data, which is a good component of a bigger program; however, if it is a requirement to encrypt data, it can hamper the Responsible Entity’s flexibility to develop a program that meets its needs in a variety of situations.

Likes 0	
Dislikes 0	

Response

Colleen Campbell - AES - Indianapolis Power and Light Co. - 3

Answer	No
Document Name	

Comment

The location where BCSI is stored is too difficult to separate from the BCSI itself. The requirements should remain focused on the storage location with the addition of key management for third party storage locations.

Likes 0	

Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
The SDT appears to have made this more convoluted and burdensome by prescribing key controls and other methods.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Agree that this is the correct approach. Greater clarity is needed within the requirements to place the requirements in the appropriate context and prevent a default fallback to the prior interpretation in the requirements.	
Likes 0	
Dislikes 0	
Response	
William Hutchison - Southern Illinois Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Comments: If this is in fact the intent of the SDT, then why is the SDT including a risk assessment of 3rd party storage solution providers? An RE would just be leveraging the 3rd party storage solution provider's hardware (physical or virtual) for a storage location.	
Likes 0	
Dislikes 0	

Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
However, we wish for clarity on this question.	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Black Hills agrees that focusing on the protection of the information rather than simply access to it is a better approach	
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	
If this is in fact the intent of the SDT, then why is the SDT including a risk assessment of 3rd party storage solution providers? An RE would just be leveraging the 3rd party storage solution provider's hardware (physical or virtual) for a storage location.	
Likes 0	
Dislikes 0	
Response	

Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
We agree with this approach but we believe this update is not backwards compatible (primarily because of the new Applicability / storage locations)	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
recommend focusing on protecting data (CIA)	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
While there is agreement to focus the security on the BCSI making the answer to the question asked a “Yes” the presence of “storage locations” in Requirement R1 defeats this SDT intention. Therefore, in its proposed form the requirement language neither aligns with nor accomplishes this stated objective	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	

Answer	Yes
Document Name	
Comment	
We agree with the approach to shift the focus of security to the BCSI; however, the SDT should consider their execution of the approach as described above.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Yes – completely agree.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NextEra	
Answer	Yes
Document Name	
Comment	
We agree with this approach but we believe this update is not backwards compatible (primarily because of the new Applicability / storage locations).	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	

Comment
OPG is in agreement with RSC provided comment

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment
However, the SDT has not completed this process in updating the previous R2, now R3 controls. Prescribing sanitization or destruction controls eliminates the ability to use encryption to restrict unauthorized access, which is a viable control. We suggest moving this back to the Objective level of preventing unauthorized access to... Or leverage the updated 1.2 language of: "Method(s) to prevent unauthorized access to BES Cyber System Information by restricting the ability to obtain and use BES Cyber System Information during storage, transit, use, and disposal, to authorized access holders." Which explicitly includes storage and disposal (and possibly eliminate R3 entirely).

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: James Mearns, 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 agrees with the shift to “System Information” (i.e. BCSI) and away from the security of the hardware. The Standard should be about Cyber Asset information and not the Cyber Assets themselves.

Likes 0	
Dislikes 0	

Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Comments: The SDT should review all the requirements to ensure that new or updated requirements do not have the unintended consequence of hindering an Entity's ability to store or use BCSI in the Cloud. See comments to question 6.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
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	
Gregory Campoli - New York Independent System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE agrees that the changes align better with the purpose of CIP-011, which reads, “To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).” Texas RE does, however, recommend the SDT consider language to permit the use of third party equipment without also removing all security obligations from equipment owned and maintained by Registered Entities since the SDT’s goal is to allow BCSI storage in equipment not owned or managed by Registered Entities (e.g. cloud providers).	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	

Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	

10. The SDT is proposing to transfer all BCSI-related requirements from CIP-004 to CIP-011 with the understanding that this will further address differing security needs between BCSI and BCS as well as ease future standard development. Do you agree that this provides greater clarity between BCSI and BCS requirements?

Michael Puscas - ISO New England, Inc. - 2

Answer	No
Document Name	

Comment

Comments: While this supports separation of controls associated with information as opposed to cyber assets/systems, it also separates controls related to access management into two standards, which may impact an entity's program organization breakdown (i.e. central approaches to access management now dealing with two standards instead of one). It would be preferable to have the access authorization/revocation requirements to be centrally located in CIP-004. Related CIP-004 requirements should sufficiently cover concerns about individual terminations at third parties.

Likes 0	
Dislikes 0	

Response

Colleen Campbell - AES - Indianapolis Power and Light Co. - 3

Answer	No
Document Name	

Comment

The CIP-004 requirements concerning BCSI revolve around authorized access to the information, that should remain in CIP-004 to maintain consistency with the current requirements and the data already collected.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

No, It is not agreed this approach provides greater clarity; rather, this approach introduces and creates ambiguity. The authorization, revocation, and review requirements should remain in CIP-004. By consolidating requirements for BCSI, the SDT is separating authorization, revocation, and review

requirements. It is better to keep the BCSI protection controls in CIP-011 and the authorization, revocation, and review requirements in CIP-004 as those are more programmatic in many cases to an organization.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

We do not agree that this provides greater clarity between BCSI and BCS requirements. The difference in Medium Impact applicability needs to be addressed by adding “with ERC” for the access requirements in R1.3 and R1.5 and these requirements need to be limited to designated storage locations of BCSI.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment
ERCOT agrees with the rationale provided regarding treating BCSI differently than Cyber Assets. However, ERCOT believes the changes would be more appropriately made by adding new parts to CIP-004, Requirements R4 and R5 that address the unique needs of BCSI. This would avoid the existence of “spaghetti requirements” and unwanted side effects of cross referencing requirements. In versions 1-3, the access requirements for BCSI were included in CIP-003. Industry provided strong feedback suggesting all access requirements should be in one location, which is why the requirements were added to CIP-004. There are entities that use a consolidated access management program to meet all regulatory requirements. Having all requirements in one location helps support this type of program. An alternative approach would be to separate the BCSI requirements into separate rows in their respective requirements of CIP-004, Requirement R4 and R5. ERCOT suggests the drafting team Consider revising Part 4.1.3 into a separate row within the CIP-004, Requirement R4 table. ERCOT believes the requirement language as written in CIP-004-6 should be retained to focus on where the information is located.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	

Comment
We do not agree that this provides greater clarity between BCSI and BCS requirements. The difference in Medium Impact applicability needs to be addressed by adding “with ERC” for the access requirements in R1.3 and R1.5 and these requirements need to be limited to designated storage locations of BCSI.

Likes 0	
Dislikes 0	

Response

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

Comment
Access requirements should remain in CIP-004.

Likes 0	

Dislikes 0	
Response	
Angela Gaines - Portland General Electric Co. - 1	
Answer	No
Document Name	
Comment	
Please see comments PGE Group 2	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE agrees with EEI's comments	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
Agree with the rationale provided of treating the BCSI different than Cyber Assets. However, the changes would be more appropriately made by adding new parts to CIP-004 R4 and R5 to address the unique needs of BCSI. This avoids the existence of "spaghetti requirements" with unwanted side effects of cross referencing requirements. In versions 1-3, the access requirements for BCSI were included in CIP-003. Industry provided strong feedback wanting all access requirements in one location, so the requirements were added to CIP-004. There are entities that use a consolidated access management program to meet all regulatory requirements. Having all requirements in one location helps support this.	

An alternate approach is to separate the BCSI requirements into separate rows in their respective requirements of CIP-004 R4 and R5. Consider making 4.1.3 into a separate row within the CIP-004 R4 table. The requirement language as written in CIP-004-6 should be retained to focus on where the information is located.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG is in agreement with RSC provided comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	No
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	

It would be more beneficial to maintain all access requirements under one Standard. Keeping access management and review programs and procedures under one Standard would reduce any confusion and decrease margins for error with compliance obligations and good sound security practices. A holistic security standard would include requirements for access approvals, revocation, and annual reviews, which is greatly important if the same department is responsible for those requirements.

Likes 0	
Dislikes 0	

Response

Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF

Answer	No
Document Name	

Comment

Alliant Energy agrees with NSRF and EEI's comments.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

Access requirements should remain in CIP-004.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NextEra

Answer	No
Document Name	

Comment

1) No because Part 1.5 will require individual terminations at third parties. It is problematic for the Entity to know when a third party's staff leaves.

2) Part 1.5 does not addess a) when the BCSI was given to the vendor and b) how to revoke one person's access?

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2

Answer	No
Document Name	

Comment

NYISO recognizes and agrees with the SDT's intent to consolidate similar issues. We recommend that the SDT pursue the maintenance of all personnel and access management requirements be contained within CIP-004-7 to better align with existing industry practices. As noted in our response to question #2, our concern with introducing access management requirements under CIP-011-3 is that it introduces a new complication, that of having to maintain similar access authorization, revocation and control measures that are currently mandated within CIP-004-7. NYISO would see this as requiring a responsible entity to be maintaining access management controls in support of two separate standards (i.e. CIP-004-7 for BCS and CIP-011-3 for BCSI), there is the potential for a single deficiency in an entity's access management program to result in non-compliance with two different NERC standards.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Please note EEI comments to questions 8 and 9 above.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	
Comment	
No. Although MISO recognizes and agrees with the SDT's intent to consolidate similar issues. We recommend that the SDT maintain all personnel and access management requirements within CIP-004-7 to better align with existing industry practices. As noted in our response to question 2, our concern with introducing access management requirements under CIP-011-3 is that it introduces a new complication, that of having to maintain similar access authorization, revocation and control measures as that in CIP-004-7. By having to maintain access management controls in support of two standards (i.e. CIP-004-7 for BCS and CIP-011-3 for BCSI), there is the potential for a single deficiency in an entity's access management program to result in non-compliance with two NERC standards.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
The standards development team should support specific requirements providing appropriate levels of security for Cloud Service Providers and 3rd Party Access. Transferring the CIP-004 BCSI requirements to CIP-011 does not address the unique issues created by storing BCSI in repositories that are not controlled by registered entities. The standards development team should draft separate requirements.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support MRO comments.	
Likes 0	
Dislikes 0	
Response	

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
We believe that this could complicate CIP access management programs. These changes seem contrary to the work completed by the V5 project team to remove the “spaghetti” requirements.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	
No because Part 1.5 will require individual terminations at third parties. It is problematic for the Entity to know when a third party’s staff leaves. Part 1.5 does not addess a) when the BCSI was given to the vendor and b) how to revoke one person’s access?	
Likes 0	
Dislikes 0	
Response	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We do not agree that this provides greater clarity between BCSI and BCS requirements. The difference in Medium Impact applicability needs to be addressed by adding "with ERC", for the access requirements in R1.3 and R1.5 and these requirements need to be limited to designated storage locations of BCSI.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
No because Part 1.5 will require individual terminations at third parties. It is problematic for the Entity to know when a third party's staff leaves Part 1.5 does not addess a) when the BCSI was given to the vendor and b) how to revoke one person's access?	
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 response found in the NSRF Comment Form	
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	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
Moving BCSI access revocation requiment from CIP-004 to CIP-011 can resulting in multiple violation of a single instance.	
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 this provides greater clarity, as it loses context. For example, the proposed R1.5 is pulled out of its CIP-004 context where it was one of five parts of an access revocation program requirement. It is then inserted into CIP-011 with no context. Read in a vacuum without the CIP-004 "Personnel and Training" standard context, Part 1.5 suddenly mentions "the individual" and "termination actions". What do those mean outside of the CIP-004 context? The requirement part prior to this was discussing vendors, so does this apply only when you terminate a vendor? Southern strongly suggests leaving the CIP-004 personnel and access management issues within CIP-004 so they don't lose vital context in a transition to CIP-011.	
Likes 0	
Dislikes 0	

Response
Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC
Answer	No
Document Name	
Comment
NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES
Likes 0	
Dislikes 0	
Response
David Jendras - Ameren - Ameren Services - 3
Answer	No
Document Name	
Comment
Ameren agrees with and supports EEI comments.
Likes 0	
Dislikes 0	
Response
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion
Answer	No
Document Name	
Comment
Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments. The current approach taken by the SDT appears too proscriptive and should remain flexiable and technology agnostic.
Likes 0	
Dislikes 0	
Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

BPA finds the strategy is reasonable but implementation of the exact verbiage needs care. Various cyber security methodologies often address cyber system protection strategies and information protection strategies separately. It's also necessary to address the BCS/BCA definition where it includes "data in the device" to clarify and make the language consistent. There could be impact on CIP-010 for change (configuration) management as the distinction between "data" and "software" is blurry in some cases. Certain best-practice managed-configuration items often referred to as "settings" (user configured inputs to the runtime parameters of a software application or operating system) that drastically affect the operation of the system are not tracked in CIP-010. These configuration items are "data in the device required for its operation" and also present an item of interest to the malicious actor and a reliability issue if they are inadvertently altered; even such things as Internet Protocol addresses and subnet masks, hostnames, Domain Name System (DNS) entries, Network Time Protocol (NTP) server addresses and similar parameters that enable reliability of a system and are not considered in CIP-010 but are covered by the current understanding of BCSI. Potential conflict between proposed requirements for protecting system data vs requirements protecting systems/devices would be very bad.

Likes 0	
Dislikes 0	
Response	

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

We do not agree that this provides greater clarity between BCSI and BCS requirements. The difference in Medium Impact applicability needs to be addressed by adding "with ERC", for the access requirements in R1.3 and R1.5 and these requirements need to be limited to designated storage locations of BCSI.

Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

N&ST sees no benefit in moving BCSI storage location access requirements from CIP-004 to CIP-011 and believes there is no need for clarification between BCSI and BCS requirements. Furthermore, N&ST believes that the impact of moving some access management requirements from CIP-004 to CIP-011 could be significant for some Responsible Entities, compelling needless modification and disruption of mature and effective CIP compliance programs.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

See NRECA submitted comments.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

While there is appreciation for the desire to “group” requirements by “applicable system”, this change fosters a bifurcated model for user and access management instead of incentivizing an enterprise program to manage risks and provisioning/deprovisioning tasks that can be unplanned and considered high frequency security operations. The SDT should resist the temptation to revert back to previously problematic constructs that created “spaghetti” in the Requirements, and maintain the construct that groups access management as a business process collectively under CIP-004. Access to BCSI also not just 3rd party and to move these requirements out from under the umbrella of user and access management in CIP-004 seems like a step backwards

Likes 0	
Dislikes 0	

Response

Vivian Moser - APS - Arizona Public Service Co. - 3

Answer	No
Document Name	
Comment	
AZPS does not necessarily agree that that the transfer of BCSI-related requirements from CIP-004 to CIP-011 provides greater clarity; however, is not opposed to aggregating all BCSI-related requirements into one standard.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
The standard does not consider nor add clarity to the third-party access and revocation requirements, a gap in security objectives as discussed in the response to Q7.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
Access management is access management keep it in CIP-004. CIP-004 includes physical and electronic access to BES Cyber Systems and BCSI. It needs to remain together. Implementing this change would cause industry to ramp-up many internal governance process changes to meet this proposed change	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	

Answer	No
Document Name	
Comment	
No, the current version of CIP-004 already provides for the identification of BCSI storage locations. Keeping all the requirements for access and revocation in one standard decreases the complexity for compliance.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
No because Part 1.5 will require individual terminations at third parties and does not address a) when the BCSI was given to the vendor and b) how to revoke one person's access?. See our comment to Question 7 While we understand the difficulty the SDT faces with leaving BCSI access requirements in CIP-004, we would prefer that all access requirements remain together within CIP-004	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC agrees with comments submitted by NRECA.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No

Document Name	

Comment

No. First, GSOC respectfully suggests that the removal of requirements from CIP-004-6 to CIP-011-3 was not authorized by the SAR for this project. In particular, the SAR explicitly stated that CIP-004 be modified and that CIP-011 be evaluated for any downstream type impacts. It did not authorize the wholesale removal of requirements from CIP-004-6 and the addition of these requirements to CIP-011-2. Accordingly, the SDT revisions go beyond the scope of the SAR as provided below:

CIP-004-6 Requirements need to be modified so management of access to BCSI is clarified to include a focus on the BCSI data and the controls deployed to limit access. In addition, the Standard should allow various methods for controlling access to BES Cyber System Information, storage location(s). … In addition to CIP-004-6 modifications, CIP-011-2 should also be evaluated for any subsequent impacts.

Second, there is significant value in the consolidation of access management requirements in 1 standard. For example, the ability of Responsible Entities to apply consolidated processes, to better ensure that minimal impacts occur as a result of revisions to standards or processes, to leverage similar or the same compliance documentation, etc. Moving only a portion of Responsible Entity's access management requirements from CIP-004 to CIP-011 places access management obligations in multiple standards, eliminated current synergies, creating confusion and process inefficiency, and increasing compliance risk. It also likely results in the requirement to modify multiple standards where access management of system scope revisions are proposed – instead of being able to implement revisions in just one standard, creating more work for SDTs and increased monitoring and commenting effort by industry.

Finally, GSOC fails to see the reliability value in segregating these requirements into 2 standards. As well, the benefits listed in the Technical Rationale are not reliability benefits, but are, rather, administrative improvements. This is highlighted by the shift to BCSI instead of locations as this shift has the likely effect of expanding access to BCSI beyond what is actually needed by personnel, exposing more BCSI to the risk of unauthorized access. For these reasons, GSOC does not support the relocation of the CIP-004 requirements associated with BCSI to CIP-011.

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

We commend the SDT for trying to consolidate all BCSI-related requirements. However, we believe CIP-004 remains the more appropriate place for the access management requirements because 1) that is where other access management requirements are located, and entities have created their access management programs based upon this, and 2) having access management requirements in two places creates the potential for multiple violations for one instance (see MRO NSRF comment).

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	

No. NRECA believes that the removal of requirements from CIP-004-6 to CIP-011-3 was not authorized by the SAR for this project. In particular, the SAR explicitly stated that CIP-004 be modified and that CIP-011 be evaluated for any downstream type impacts. It did not authorize the wholesale removal of requirements from CIP-004-6 and the addition of these requirements to CIP-011-2. Accordingly, the SDT revisions go beyond the scope of the SAR as provided below (emphasis added):

CIP-004-6 Requirements need to be modified so management of access to BCSI is clarified to include a focus on the BCSI data and the controls deployed to limit access. In addition, the Standard should allow various methods for controlling access to BES Cyber System Information, storage location(s). … In addition to CIP-004-6 modifications, CIP-011-2 should also be evaluated for any subsequent impacts.

Additionally, there is significant value in the consolidation of access management requirements in a single standard. For example, the ability of Responsible Entities to apply consolidated processes, to better ensure that minimal impacts occur because of revisions to standards or processes, to leverage similar or the same compliance documentation, etc. Moving only a portion of Responsible Entity's access management requirements from CIP-004 to CIP-011 places access management obligations in multiple standards, eliminates current synergies, creates confusion and process inefficiencies, and increases compliance risk. It also likely results in the requirement to modify multiple standards where access management of system scope revisions are proposed – instead of being able to implement revisions in just one standard, creating more work for SDTs and increased monitoring and commenting effort by industry.

Finally, NRECA fails to see the reliability value in segregating these requirements into 2 standards. As well, the benefits listed in the Technical Rationale are not reliability benefits, but are, rather, administrative improvements. This is highlighted by the shift to BCSI instead of locations as this shift has the likely effect of expanding access to BCSI beyond what is needed by personnel, exposing more BCSI to the risk of unauthorized access. NRECA does not support the relocation of the CIP-004 requirements associated with BCSI to CIP-011.

Likes 0	
Dislikes 0	
Response	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	

AECI supports comments filed by NRECA

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	
Fragmenting user access across two standards is a regressive action that negates a substantive uplift that NERC adopted in the version 5 standards. Suggest retain all user access controls in CIP-004.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
If specific access controls are deemed necessary, Seattle prefers that access requirements remain grouped in CIP-004, and furthermore recommends alignment of termination timing for BCSI from “calendar day” to “24 hours” as is consistent with timing for other termination requirements. Even better to Seattle would be to drop specific access requirements for BCSI and/or BCSI storage locations from either of CIP-004 or CIP-011, and left up to each entity to specify in their risk-based BCSI security plan. Expectations and guidance could be provided in the Measures and technical documents.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
We disagree with moving requirements for access to BCSI from CIP-004-6 to CIP-011-3 (see our response in Question 2) and we havn’t seen any security needs for this change.	
Likes 0	

Dislikes 0	
Response	
Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
This places access management outside of CIP-004.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy support the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

Not until the difference in Medium Impact applicability is addressed (add “with ERC”), and these requirements are limited to designated storage locations of BES CSI.

Per our response to Question 2, we disagree with moving requirements for access to BCSI from CIP-004-6 to CIP-011-3. We appreciate the attempt to streamline Requirements associated with BCSI by placing all related compliance activities solely within the CIP-011-3 Standard. However, by doing so Responsible Entities would be subject to the potential of having multiple compliance issues with one failed compliance activity as a result of the overlapping NERC CIP Standards.

To describe the scenario we offer the following: If an Entity were to have an employee, contractor or vendor with approved access to BCSI and no other physical or logical access to BES Cyber Systems or Cyber Assets and that employee left the company then we would be required to revoke access by the end of the next calendar day, per CIP-011-3 R1.5. If we were to have a miss and not revoke by the next calendar day then we would need to self-report on CIP-011-3 R1.5. If we have an employee with access to CIP Cyber Systems or Cyber Assets and not to BCSI and failed to remove the employee’s access then we would have to self-report on CIP-004-7 R5. If we have an employee that has access to both BES Cyber Systems and to BCSI and we fail to remove access in a timely manner then we have violations for both CIP-004-7 R5 and for CIP-011-3 R1. This isn’t an issue today because all access violations are rolled up to CIP-004-6 R5 but by separating them into two Standards we would be required to report on both and thus exposing us to multiple possible violations whereas today it would only be one.

Additionally, many Responsibly Entities’ Access Control procedures are written under CIP-004-6 - Access Control procedure. Everything an employee would need to know about their access control responsibilities would be located in a single document. This change would either create a potential compliance risk by breaking access controls up into separate documents or cause entities to perform significant changes to how they document their compliance procedures.

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	

Grouping by control type rather than CIP standard number is preferred. Access controls in many different areas of the standard does not add clearity.

Likes 0	

Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy does not agree with the transfer of all BCSI-related requirements from CIP-004 to CIP-011. Duke Energy concludes that moving access revocation requirements from CIP-004 to CIP-011 will create the potential for access revocation of an individual entity violating requirements in two separate standards.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	No
Document Name	
Comment	
There are two separate ways of evaluating this question. On one hand, it seeks to create a common place to include requirements on information protection. On the other hand, it breaks the previous approach to consolidate all access authorization, provisioning, revocation, and deauthorization. By moving these requirements, it also potentially changes a single violation for CIP-004 R4 or R5 into multiple violations.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, 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 agrees with the shift of BCSI access authorization and revocation from CIP-004 to CIP-011. This allows an entity the option to have different processes in place for granting and removing access to BCSI if they desire and removes the implied requirement of having a Personnel Risk Assessment (PRA) executed before access to BCSI is granted if the entity does not what to make that a requirement in their environment.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

However, the SDT should modify the applicability in CIP-011-3 requirements to align with CIP-004.

Likes 0	
Dislikes 0	

Response

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members

Answer	Yes
Document Name	

Comment

SNPD supports this change. CIP-004 should address BCS while CIP-011 should address BCSI (physical vs logical access). Mixing access and storage requirements across multiple CIP standards is confusing and increases the likelihood for mismanagement.

Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	

Response

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3

Answer	Yes
Document Name	

Comment
Yes, however it is worth acknowledging that R3 applies to disposal/redeployment of cyber assets, not BCSI. Additionally, we suggest making separate requirements for BCSI on premises versus in the cloud. This way there can be no implication that something new is required for BCSI on premises, such as it appears currently with key management (R2).

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
Yes it will make changes to CIP-011 easier in the future, but it also allows for ease of changes in the future which makes it easier to include Low Impact. This was brought up on the webinar that the scope of the SAR does not include Low Impact, but this change will easily allow changes to the standard to include Low Impact without unintended consequences to other standards/requirements.

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3	
Answer	Yes
Document Name	

Comment
AEP agrees these changes have the potential to provide greater clarity surrounding BSCI and BCS. However, please see AEP’s comments to questions #8 and #9.

Likes 0	
Dislikes 0	

Response

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

Document Name	
Comment	
Black Hills agrees that placing all the BCSI requirements into one standard provides clarity. However, we think it would be beneficial to modify the language taken from CIP-004, making it less rigid.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Overall yes; however, some third party issues remain to be addressed. See NPCC RSC comments.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Yes, however it is worth acknowledging that R3 applies to disposal/redeployment of cyber assets, not BCSI. Additionally, Tri-State suggests making separate requirements for BCSI on premises versus in the cloud. This way there can be no implication that something new is required for BCSI on premises, such as it appears currently with key management (R2).	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	Yes

Document Name	
Comment	
Moving the BCSI requirements from CIP-004 to CIP-011 as proposed is OK with MEAG. It doesn't matter if the BCSI requirements are all in 1 standard or multiple standards.	
Likes 0	
Dislikes 0	
Response	
William Hutchison - Southern Illinois Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Comments: Yes it will make changes to CIP-011 easier in the future, but it also allows for ease of changes in the future which makes it easier to include Low Impact. This was brought up on the webinar that the scope of the SAR does not include Low Impact, but this change will easily allow changes to the standard to include Low Impact without unintended consequences to other standards/requirements.	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
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	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	

See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	

11. The SDT increased the scope of information to be evaluated by including both Protected Cyber Assets and all Medium Impact (not just Medium Impact Assets with External Routable Connectivity). Are there any concerns regarding a Responsible Entity attempting to meet these proposed, expanded requirements?

William Hutchison - Southern Illinois Power Cooperative - 1

Answer	No
Document Name	

Comment

Comments: Yes, an Entity without ERC today will now be required to have an information protection program which could have a major impact. What is the risk sought to be reduced here? There is not a possibility to use a site without ERC as a pivot point, so the likelihood of a site without ERC being used in a cyber-attack is incredibly low. Increasing the scope here only furthers the point from question 10 on easily increasing scope in the future.

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

This will add workload that may may not be justified by risk. Devices without ERC have less IT security risk than routable devices.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	

Comment

Removing the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 R4.1, R4.4, R5.3 when moved them to CIP-011-3 R1.3, R1.4, and R1.5 is unacceptable. This “with ERC”deletion expands the scope of CIP-004 R4 and R5 requirements signicantly. After this scope expansion, CIP-004 R4 and R5 requirements will not only apply to all locations of BCSI pertaining to Medium Impact BES Cyber Systems, but also apply to all Medium Impact BCS since the Medium Impact BCS contains BCSI. This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a considerable and sufficient protection in and of itself and this is why the current CIP-004 R4 and R5 don’t apply to Medium Impact BCS without ERC.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

Seattle is concerned about the expansion of scope introduced by these changes. Are they warranted from a security standpoint, given that BSCI about a Medium substation without ERC, for example, likely presents less risk to the BES than the network information about a Low substation with ERC (which is not even covered at all). Considerable additional resources will need to be expended to protect BCSI that may not present a significant security risk, apparently only for the reason of consistency in wording. See also response to Question 2, above.

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1

Answer	No
Document Name	

Comment

It would be helpful if SDT provide some rationale for expanding the applicability to PCA. This expansion is not reflected in the Standard Authorization Request. We need to ensure that additional compliance burden pays off in mitigating the security risk.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	
Comment	
AECI supports comments filed by NRECA	
Likes 0	
Dislikes 0	
Response	

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	
Comment	

Yes. NRECA believes the removal of requirements form CIP-004-6 to CIP-011-3 was not authorized by the SAR for this project. The SAR explicitly stated that the purpose or goal of the project was "[c]larifying the CIP requirements and measures related to both managing access and securing BES Cyber System Information." Further, the scope of the SAR did not make any mention of scope expansion. In fact, the SAR explicitly provided for modifications to "clarify" existing access management requirements for BCSI. Accordingly, because the SAR did not contemplate or authorize scope expansion relative to asset applicability, the SDT revisions go beyond the scope of the SAR as provided below (emphasis added):

CIP-004-6 Requirements need to be modified so management of access to BCSI is clarified to include a focus on the BCSI data and the controls deployed to limit access. In addition, ***the Standard should allow various methods for controlling access to BES Cyber System Information, storage location(s)***. The focus must be on BCSI and the ability to obtain and make use of it. This is particularly necessary when it comes to the utilization of a third party's system (e.g. cloud services). The current Requirements are focused on access to the "storage location", but should consider management of access to BCSI while in transit, storage, and in use. In addition to CIP-004-6 modifications, *CIP-011-2 should also be evaluated for any* ***subsequent*** *impacts*.

Further, NRECA notes that PCAs currently do not require authorization for access in CIP-004. If no access authorization is required to access the asset itself, it is unclear as to why authorization would be required to obtain access to information about a system for which no access authorization is required. This contradiction is not addressed within the Technical Rationale and should be addressed by the SDT to ensure that there is an appropriate identification of risk associated with the recommendation to add PCAs to CIP-011.

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	
Agree with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

Yes. First, GSOC respectfully suggests that the removal of requirements form CIP-004-6 to CIP-011-3 was not authorized by the SAR for this project. In particular, the SAR explicitly stated that the purpose or goal of the project was "[c]larifying the CIP requirements and measures related to both managing access and securing BES Cyber System Information." Further, the scope of the SAR did not make any mention of scope expansion. In fact, the SAR explicitly provided for modifications to "clarify" existing access management requirements for BCSI. Accordingly, because the SAR did not contemplate or authorize scope expansion relative to asset applicability, the SDT revisions go beyond the scope of the SAR as provided below (emphasis added):

CIP-004-6 Requirements need to be modified so management of access to BCSI is clarified to include a focus on the BCSI data and the controls deployed to limit access. In addition, ***the Standard should allow various methods for controlling access to BES Cyber System Information, storage location(s)***. The focus must be on BCSI and the ability to obtain and make use of it. This is particularly necessary when it comes to the utilization of a third party's system (e.g. cloud services). The current Requirements are focused on access to the "storage location", but should consider management of access to BCSI while in transit, storage, and in use. In addition to CIP-004-6 modifications, *CIP-011-2 should also be evaluated for any* ***subsequent*** *impacts*.

Further, GSOC notes that PCAs currently do not require authorization for access in CIP-004. If no access authorization is required to access the asset itself, it is unclear as to why authorization would be required to obtain access to information about a system for which no access authorization is required. This contradiction is not addressed within the Technical Rationale and should be addressed by the SDT to ensure that there is an appropriate identification of risk associated with the recommendation to add PCAs to CIP-011.

Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	

SMEC agrees with comments submitted by NRECA.

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

Yes, an Entity without ERC today will now be required to have an information protection program which could have a major impact. What is the risk sought to be reduced here? There is not a possibility to use a site without ERC as a pivot point, so the likelihood of a site without ERC being used in a cyber-attack is incredibly low. Increasing the scope here only furthers the point from question 10 on easily increasing scope in the future.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

This seems to defeat the SDT's stated intention to focus the security on the BCSI; therefore, in its proposed form the requirement language neither aligns with nor accomplishes this stated objective

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

See NRECA submitted comments.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST does not have any concerns with the proposed expansion of CIP-011 to include PCAs. N&ST notes that the current, enforceable CIP-011-2 is already applicable to all Medium Impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC

Answer	No
Document Name	

Comment

NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Oncor does not agree with the scope expansion unless the SDT provide justification that pay off additional burden in mitigating the security risk.

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. Additionally, SDG&E would like to comment on CIP-011-3 requirement's proposed inclusion of all Medium-Impact BCS, regardless of ERC. The current CIP-004-6 R4.4 requirement specifies applicability for only High Impact BCS and Medium Impact BCS with ERC. The new CIP 011-3 brings all BCSI in scope regardless of ERC in Medium-Impact Sites. This change is significant and overburdensome to sites that don't currently fall into this category of BCSI.	
Likes 0	
Dislikes 0	
Response	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	

We are concerned because of access management associated with Medium Impact.

This expansion is not backwards compatible

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	

Comment

No – PCA may also contain BCSI.

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2

Answer	No
Document Name	

Comment

PCA may also contain BCSI.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

We may in the future.	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
We may in the future.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	

Removing the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems from CIP-004-6, when moved to CIP-011-3 R1.3, greatly expands the scope of this requirement. This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a considerable protection.

The scope is also expanded significantly by changing the former CIP-004 requirements to apply to all BCSI, not just designated storage locations of BCSI.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: James Mearns, 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 has concerns regarding the addition of PCA and the benefit of including them compared to the effort of identifying and protecting BCSI related to PCA. As noted in Question 5, PG&E would like the SDT to articulate the reason for the addition of PCA since there is no information in the Technical Rationale document to warrant its addition.

Regarding the inclusion of all Medium Impact BCS, PG&E believes this is an appropriate modification since the BCSI information for these Cyber Assets could be used to compromise those Cyber Assets if physical access is gained.

Likes 0	
Dislikes 0	

Response

Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
SunPower supports Duke Energy's comments. This creates a possibility of multiple violations as opposed to a single violation in the original CIP-004 Standard.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colleen Campbell - AES - Indianapolis Power and Light Co. - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
We are concerned with scope creep. What problem are we trying to solve?	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy is concerned that increasing the Applicability of the Requirements to include the addition of PCAs and all Medium Impact BCS would require significant efforts to modify technical, administrative, and operational controls, compliance processes, and evidentiary documentation. Duke Energy suggests to consider surveying Responsible Entities to assess how many PCAs and Medium Impact BCS would now need to comply with CIP-011-3 and at what cost vs. the potential increase in Reliability to the BES.	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	Yes
Document Name	
Comment	
More clarity is needed.	
Likes 0	
Dislikes 0	
Response	

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	

Removing the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 R4.1 when moved to CIP-011-3 R1.3, is unacceptable. This deletion greatly expands the scope of this requirement. This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a considerable and sufficient protection in and of itself.

The scope is also expanded significantly by changing the former CIP-004 requirements to apply to all BCSI, not just designated storage locations of BCSI.

Lack of ERC also renders BCSI pertaining to Medium Impact BES Cyber Systems outside the scope of R1 Part 1.2, as any such information, if obtained, cannot be used remotely, as there is no remote access to the Cyber Systems. These Cyber Systems can only be compromised by breaching physical security, in which case this standard provides no protection.

Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	

The addition of PCAs is overburdensome. By definition, PCAs do not have a 15 minute impact on the reliability of the BES. They are not a part of a BCS and should not be considered BCSI.

Likes 0	
Dislikes 0	
Response	

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Xcel Energy support the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	Yes
Document Name	
Comment	
Support the MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Tri-State does not agree with the scope expansion, as the risk associated with these added assets is much lower. This does not conform to the risk-based approach that the ERO has been striving to. The SDT would need to provide justification for scope expansion, especially given this was not in scope of the SAR.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	

Suggest retaining existing scope that includes exclusions for Medium without ERC. The security posture of a system without ERC substantively decreases the value of BCSI for remote attack scenarios, thus greatly reducing the value of that information to a potential adversary.

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3

Answer	Yes
Document Name	

Comment

AEP agrees with EEI, and does not support the addition of PCAs and Medium Impact Assets without ERC because the SDT has not adequately described the risks or provided an explanation that justifies the expanded compliance burdens for entities. These changes go beyond the scope of the SAR and improperly expands the scope of protections beyond the currently approved CIP Reliability Standards.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

We are concerned because of additional effort that imposing access management associated with BCSI for Medium Impact BCS (without ERC) and PCAs
While IESO has only High Impact BCS, further analysis would need to be done to determine the amount of the impact on Ontario market participants where this applicability would apply

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper

Answer	Yes
Document Name	

Comment

The proposed changes will add a considerable amount of work to any utilities that have Medium Impact Assets without ERC which may not be justified by risk. Devices without ERC have less IT security risk than routable devices.

Likes 0	
Dislikes 0	

Response

Vivian Moser - APS - Arizona Public Service Co. - 3

Answer	Yes
Document Name	

Comment

AZPS is concerned that the proposed expansion of CIP-011-3 to include Protected Cyber Assets and all Medium Impact Assets is unnecessary and may be overly burdensome on Responsible Entities. AZPS believes the protections already afforded to these assets through the implementation of CIP-005-5 and CIP-006-6 are sufficient to protect against any unauthorized “use” of BCSI.

Likes 0	
Dislikes 0	

Response

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3

Answer	Yes
Document Name	

Comment

Tri-State G&T does not agree with the scope expansion, as the risk associated with these added assets is much lower. This does not conform to the risk-based approach that the ERO has been striving to. The SDT would need to provide justification for scope expansion, especially given this was not in scope of the SAR.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	

Comment
Removing the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 R4.1 when moved to CIP-011-3 R1.3greatly expands the scope of this requirement. This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a considerable and sufficient protection in and of itself. The scope is also expanded significantly by changing the former CIP-004 requirements to apply to all BCSI, not just designated storage locations of BCSI. Having a lack of ERC also renders BCSI pertaining to Medium Impact BES Cyber Systems outside the scope of R1 Part 1.2, as such information, if obtained, cannot be used remotely, as there is no remote access to the Cyber Systems. Information pertaining to these Cyber Systems can only be used to compromise them by breaching physical security, in which case the CIP-011 standard provides no protection.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment
As always, the cyber risk is not well-addressed by rating cyber systems by association with physical BES assets and facilities. The risk from cyber attack is the speed of exploit. Automation and vulnerabilities on one machine can be exploited and spread exponentially through networks infecting all other assets within a similar security profile or to which an unprotected or poorly secured connection exists. So the cyber risk and the impact to the particular BES asset to which it is attached are not a good proxy for each other. The risk to the BES of lots of poorly secured cyber assets is that in concert they can have a disparately large impact to multiple BES assets. Aggregate attacks on low impact cyber assets can equate to a moderate level of impact, and likewise attacks on (individually) medium impact assets can have a high impact when aggregated across a large number of such facilities.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	

Comment

Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments. The potential expansion of the scope to these assets appears to be poutside the scope of the original SAR.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	Yes
Document Name	

Comment

Ameren agrees with and supports EEI comments.

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

This scope expansion was **not** in the SAR and the Technical Rationale states it was added, but gives no rationale as to why it was added. What risk is being mitigated that justifies an increase in effort and cost? A case can be made that PCAs are already covered in the existing language since network diagrams and lists of all network clients are already included in the definition of BCSI. We suggest the SDT include a rationale for the addition in the Technical Rationale document and appropriately outline the risk that is being addressed.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes

Document Name	
Comment	
ITC supports the response found in the NSRF Comment Form	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
We are concerned because of access management associated with Medium Impact would bring into scope a large number of information related to medium impact substations .	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Removing the qualifying language "with ERC" from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 R4.1 when moved to CIP-011-3 R1.3, greatly expands the scope of this requirement. This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a considerable and sufficient protection in and of itself. *The scope is also expanded significantly by changing the former CIP-004 requirements to apply to all BCSI, not just designated storage locations of BCSI.* *Having a lack of ERC also renders BCSI pertaining to Medium Impact BES Cyber Systems outside the scope of R1 Part 1.2, as such information, if obtained, cannot be used remotely, as there is no remote access to the Cyber Systems. Information pertaining to these Cyber Systems can only be used to compromise them by breaching physical security, in which case the CIP-011 standard provides no protection.*	

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	Yes
Document Name	

Comment

As described in the SAR, the changes were to add the ability to allow entities to use cloud services and to clarify the requirements and measures related to access and securing BCSI. We are unsure why the changes included expanding the scope to all Medium Impact BCS and PCAs. If approved as written, 18 months will not be sufficient time to implement this across this large number of new assets, locations and information. Additionally, an asset that has no impact on the BES and just resides within the same ESP as a BCS, a PCA, does not (by default) have BCSI.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Please provide more clarity on the phrase "System information pertaining to". This needs to be well defined and understood. There may be many systems that are associated with systems that may or may not house BCSI.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

As a note, CIP-011-2 already applied to all Medium Impact whether or not External Routable Connectivity existed.

Adding PCA is a concern because it could be a major new effort unsupported by existing resources with expertise in OT, not IT, assets. Existing storage locations, especially for substation BCS, PACS, and EACMS may be using a file-based version control system that may only be configured and capable of handling a small number of text or firmware files. This system may not not be amenable to storing more complex configurations of a local PCA such as a terminal or server running Windows.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

EEI cannot support the addition of PCAs and Medium Impact Assets without ERC because there has not been an adequate identification of the risks or an explanation for the expanded scope. These changes go beyond the scope of the SAR and expands the scope of protections beyond the currently approved CIP Reliability Standards. The SDT should limit the applicability of BCSI to what is currently approved in CIP-011-2. If the SDT is aware of any reliability gaps, it should develop a white paper to support their concerns and develop a revised SAR for approval.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NextEra

Answer	Yes
Document Name	

Comment

1. We are concerned because of access management associated with Medium Impact.

1. This expansion is not backwards compatible.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
1. BC Hydro considers that additional guidance on the interpretation of what constitutes BCSI within either the Standard or the definition of BCSI is needed for a more consistent framework across the industry. 2. With the expansion of scope to PCAs, BC Hydro requests that the language of the Standard includes provisions that limit the scope of authorization requirements only to information disseminated after the effective date of the standard, and clarity that audits of previously released information is not required.	
Likes 1	BC Hydro and Power Authority, 5, Hamilton Harding Helen
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	
SNPD does not understand what the new language is trying to achieve. We believe we understand and would likely choose to agree with the proposed change, but the language does not appear to provide the necessary descriptive clarity to differentiate between whether the standard is attempting to govern ALL PCA within medium facilities or just PCA with external connectivity? If the intent is ALL, please state so clearly.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI’s comments.	
Likes 0	
Dislikes 0	

Response
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3
Answer	Yes
Document Name	
Comment
See Steven Toosevich's comments.
Likes 0	
Dislikes 0	
Response
Constantin Chitescu - Ontario Power Generation Inc. - 5
Answer	Yes
Document Name	
Comment
OPG is in agreement with RSC provided comment
Likes 0	
Dislikes 0	
Response
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2
Answer	Yes
Document Name	
Comment
PGE agrees with EEI’s comments
Likes 0	
Dislikes 0	
Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
While the identification of BCSI has not increased in scope, the identification of BCSI storage locations has. This will add burden to entities that have many Medium Impact systems with no ERC. Additionally, the R1 Part 1.2 requirement language as written seems to make even authorized access impossible.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	
Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Removing the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems from CIP-004-6, when moved to CIP-011-3 R1.3, greatly expands the scope of this requirement. This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a considerable protection.	

The scope is also expanded significantly by changing the former CIP-004 requirements to apply to all BCSI, not just designated storage locations of BCSI.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	Yes
Document Name	

Comment

There are several expansions of scope built into this proposed revision. CIP-004-6 Part 4.4 is applicable to only Medium Impact BES Cyber Systems with ERC. The ERC qualifier is removed as part of CIP-011-3 Part 1.3. While most Responsible Entities likely take care to protect BCSI to one degree or another, there is not a compliance threshold for authorizing access to BCSI associated with Medium Impact BES Cyber System without ERC. This proposed change increases the burden on Responsible Entities. Additionally, PCAs are introduced as associated devices in this proposed revision. Again, most Responsible Entities are likely protecting much of the information, and this creates a new compliance threshold and new compliance burden that Responsible Entities will have to bear. A signicant effort will be required to evaluate processes and procedures, to re-evaluate devices, provide training, update and change technologies that are used to authorize and approve access. There are concerns that this will take more than minimal effort to accommodate these changes without commensurate security benefits.

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

Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Angela Gaines - Portland General Electric Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	

12. In looking at all proposed recommendations from the SDT, are the proposed changes a cost-effective approach?

Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
SunPower believes the cost of meeting the Standard will be greater by instituting key controls and other prescribed processes that are unnecessary. It increases workload greatly.	
Likes 0	
Dislikes 0	
Response	
Colleen Campbell - AES - Indianapolis Power and Light Co. - 3	
Answer	No
Document Name	
Comment	
The key management section needs to be better defined to show a difference between on premise and third party storage of BCSI. Solutions to the key management issue may prove costly depending on the scope of where it will need to be used.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
The proposed changes significantly increase the compliance and documentation burden without a commensurate increase in security. We believe the standard revisions will increase the risk of non-compliance due to some of the proposed requirements having impossible evidencing requirements.	

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: James Mearns, 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 indicates the move of access authorization and revocation from CIP-004 to CIP-011 and inclusion of key management are appropriate in addressing the protection of BCSI. There could be increased costs related to key management if an entity does not have that current capability for key management but does not believe there would be any cost increase if an entity currently has a key management program.

For the addition of PCA, PG&E has concerns related to the benefit of their inclusion compared to the administrative burden of identifying and protecting that BCSI. As noted in Question 5, PG&E would like the SDT to articulate the reason for the addition of PCA to help determine if it should be covered by the Standard.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Light Company believe there is a more cost-effective approach as set forth in EEI's comments.

Likes 0	
Dislikes 0	

Response

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

Answer	No

Document Name	
Comment	
As noted elsewhere, ERCOT believes some of the proposed changes may be administratively burdensome and that more cost-effective solutions may be available. Recognizing that complying with new regulations will lead to increased costs, a more cost-effective approach may be to focus on less prescriptive controls and focus more on objective or outcome based changes. ERCOT also notes that it is difficult to determine cost-effectiveness absent a complete draft standard.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
The proposed changes significantly increase the compliance and documentation burden without a commensurate increase in security. We believe the standard revisions will increase the risk of non-compliance due to some of the proposed requirements having impossible evidencing requirements.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
If it where cost effective it would NOT be so prescriptive. Please include the real cost in the estimates maybe $350K/year+? Remember the WECC Poka-Yoke webinar. Thorough project controls analysis; whatever can fail plan, will fail; so plan for cost of finding failures and fixing failures, then doing it again until no failures, include all this work WECC discusses in their webinar in cost estimates.	
Likes 0	
Dislikes 0	
Response	

James Brown - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
As noted above, some of the proposed changes are administratively burdensome and a more cost-effective solution may be available. Recognizing that complying with new regulations will lead to increased costs, a more cost-effective approach may be to focus on less prescriptive controls and instead be more focused on objective or outcome based changes. Additionally, it is difficult to determine cost effectiveness with the first draft of a standard.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
An evaluation would be needed to determine, but this proposal would likely add costs and does not appear to be cost effective as written. This recommendation will require additional time, attention, and coordination between several departments and subject matter experts.	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with NSRF’s comments.	
Likes 0	
Dislikes 0	
Response	

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
No, the proposed changes do not meet the goal of enabling (relatively) easy vetting and procurement of cloud services or efficient use of cloud services without the need for onerous local key management, and will likely not result in adoption of cloud services for BCSI due to the increased resources required to vet, secure, and maintain BCSI in the cloud. Reciprocal federal certifications, such as those described in the response to Question 3, would greatly alleviate the resources required for small and medium sized Entities.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
If it where cost effective it would NOT be so prescriptive. Please include the real cost in the estimates maybe $350K/year+? Remember the WECC PokaYoka webinar. Though project controls analysis. Whatever can fail plan for those high costs in esimate too?	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro estimates that significant costs will likely be incurred, particularly in relation to R2 of CIP-011-3. Also the use of vendors will lead to significant costs relating to risk assessments under R1.4. If vendors need to adhere to entity imposed Vendor controls, the costs may be passed back to the responsible entity. More cost effective approach would be to establish an industry accceptable standard for vendors and, if they meet these criteria, this would negate vendor risk assessments as part of reliability standard requirements. This could be done by creating a list of certified vendors for entity use.	

Likes 1	BC Hydro and Power Authority, 5, Hamilton Harding Helen
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2

Answer	No
Document Name	

Comment

As noted in our response to questions 6 and 8 above, some of the proposed changes are administratively burdensome where more efficient and cost-effective solutions may be available. Recognizing that complying with new regulations will lead to increased costs; it would seem that a less prescriptive method favoring an objective / outcome-based requirement would be a better approach. Cryptosystems and key management may be cost prohibitive for many organizations.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Unintentionally, check a response to question 12. EEI offers no response to question 12.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	

Comment

No. As noted in our response to questions 6 and 8 above, some of the proposed changes are administratively burdensome where more cost-effective solutions may be available. Recognizing that complying with new regulations will lead to increased costs, a more cost-effective approach may be to focus on less prescriptive methods in favor of objective / outcome-based requirements.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support MRO comments.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	No
Document Name	

Comment

We believe that the proposed changes, which include the changes for cloud-based solutions and the increased scope for Medium Impact and PCAs, are not a cost-effective approach.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

The changes included will require additional cost to every entity in North America, primarily through increased staff needed for compliance management. Also, the additional cost associated with the change to Medium Impact expanded scope.

Likes 0	
Dislikes 0	

Response

Ayman Samaan - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

The proposed changes significantly increase the compliance and documentation burden without a commensurate increase in security.

We belive the standard revisons will increase the risk of non-compliance due to some of the proposed requirements having impossible evidencing requirements.

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 response found in the NSRF Comment Form	
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. SDG&E believes the new requirements will increase costs for the Responsible Entities.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
See response to question #11.	
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 agrees with other industry organizations, particularly NSRF, where the proposed changes will significantly increase the compliance and documentation burden without a commensurate increase in security.	
Likes 0	
Dislikes 0	
Response	
Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC	
Answer	No
Document Name	
Comment	
NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy does not have enough information to make an informed cost effectiveness conclusion.	
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

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

The proposed changes significantly increase the compliance and documentation burden without a commensurate increase in security.

We belive the standard revisons will increase the risk of non-compliance due to some of the proposed requirements having impossible evidencing requirements.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST believes the costs associated with moving CIP-004 access management requirements to CIP-011, with changing the objects of access management from BCSI storage locations to BCSI, with being required to perform annual risk assessments of 3rd-party BCSI storage vendors, and with implementing prescriptive key management program requirements could be significant. At the same time, N&ST believes these proposed changes would neither achieve the SDT’s stated goals nor improve the security of BES Cyber System Information.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	
Comment	
See NRECA submitted comments.	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3	
Answer	No
Document Name	
Comment	
Tri-State expects the proposed changes, as drafted, to be costly. For example, Part 2.2 prescribes a segregation, without any consideration of controls, that could 1) prevent an entity from utilizing a cloud solution and instead having to pay the more expensive rate for on premise solution, 2) prevent an entity from being able to fully implement into a cloud solution (which means managing and paying for both cloud and on premise environments), or 3) result in a substantial increase in costs associated with managing keys on premise with additional staff, or by a 3rd party.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
Given the duplicity of these proposed modifications with other current or future enforceable standards, these revisions are too prescriptive and introduce undue administrative burden without accomplishing the SDT’s stated objectives. In addition, moving CIP-004 requirements into CIP-011 has unintended consequences and does not achieve the perceived efficiency.	
Likes 0	
Dislikes 0	
Response	

Vivian Moser - APS - Arizona Public Service Co. - 3	
Answer	No
Document Name	
Comment	
AZPS is unable to make a determination of cost effectiveness at this time due to uncertainties in the requirements as currently drafted.	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
The proposed changes are not a cost-effective approach for a utility that does not ERC. These organizations will now have to look at their Medium Impact Asset documentation and decide what will become BCSI and then create storage locations for the information.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
The potential costs of the Part R1.4 vendor controls may not produce an effective result. In addition, the submitted feedback to Standards Efficiency Review tends to question the value of annual reviews for the sake of a review. We would prefer a specific trigger or sets of triggers for reviews.	
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	
Because of the increases in scope of the standard this could have significant cost increases for REs making using 3rd party storage solutions cost ineffective.	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC agrees with comments submitted by NRECA.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
The proposed changes increase compliance activities and burden without the likelihood of an associated increase in reliability or security. Further, several of the proposed changes would result in infeasible and impracticable compliance obligations. For example, as discussion above in GSOC's response to question #, the proposed revisions regarding the identification of BCSI would require a demonstration that all system information has been evaluated for classification as BCSI. Such is infeasible. Another example is the revocation requirements set forth in requirement R1.5, which, when coupled with the new requirements around identification of BCSI, would require that Responsible Entities prove that they successfully revoked access to every, possible, individual piece of BCSI. Such is not feasible and is a paper exercise that is not cost-effective or beneficial to reliability or security. Further, ambiguity around the term "sanitization" raises concerns that it unnecessarily raises the bar and reduce flexibility regarding what needs to be done to an asset prior to reuse of disposal. This creates uncertainty and increases the burden of compliance on Responsible Entities for no ostensible enhancement to reliability or security. This proposed revision and its consequences further impact overall cost-effectiveness of the proposed revisions as entities that cannot segregate storage media from the overall asset will either have to sanitize the entire device or destroy the entire device, neither of which results in a cost-effective solution for entities. 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.	

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

Agree with MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

Based on our comments above, the proposed revisions do not propose substantive enhancements to security or reliability that would justify additional costs/resources.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

AECI supports comments filed by NRECA

Likes 0	
Dislikes 0	

Response	
Kent Feliks - AEP - 3	
Answer	No
Document Name	
Comment	
AEP does not feel as though these changes are a cost effective approach. These changes will require additional training for employees due to requirements shifting to a different standard. Additionally, managing cloud service encryption and keys can be potentially expensive. However, AEP recognizes that cost-related circumstances vary by Responsible Entity.	
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	
This has the effect of ever increasing scope to include anywhere an instance of BCSI may reside, whether in a physical and/or logical form. If an individual were to create a paper copy of a BCSI, the entity would be obligated to track that paper until its destruction to ensure that it managed access to the BCSI. The additional review, controls, risk assessment, and significant expansion of the scope of this compliance obligation as written would have a high cost for the entity.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State expects the proposed changes, as drafted, to be costly. For example, Part 2.2 prescribes a segregation, without any consideration of controls, that could 1) prevent an entity from utilizing a cloud solution and instead having to pay the more expensive rate for on premise solution, 2) prevent an	

entity from being able to fully implement into a cloud solution (which means managing and paying for both cloud and on premise environments), or 3) result in a substantial increase in costs associated with managing keys on premise with additional staff, or by a 3rd party.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

Seattle is unconvinced that the proposed changes represent a cost-effective approach, given the complexity of the required approaches; the unresolved questions about “obtain and use,” storage locations, R2 conflict with CIP-013, etc; and the prescriptive nature of new requirements R1.4, R1.5, and R2 that once again presume certain (although different) technology concepts that will no doubt soon become obsolete.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	

Comment

The proposed changes significantly increase the compliance and documentation burden without a commensurate increase in security. The requirements are beyond the goals of SAR. The goals of SAR are to clarify the CIP requirements and measures related to both managing access and securing BES Cyber System Information and clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

Likes 0	
Dislikes 0	

Response

Jeremy Voll - Basin Electric Power Cooperative - 3

Answer	No
Document Name	

Comment

Support the MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
Refer to question 11.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
The proposed changes significantly increase the compliance and documentation burden without a commensurate increase in security. The requirements are going well above and beyond the SAR, and as written requires more controls than are necessary to mitigate risks. For example, peforming vendor risk assessments at least once every 15 calendar months may not be commensurate with the low level of risk a vendor may pose, or there are no changes in the vendors practices that would warrant another assessment.	
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 standards may not reach the goal of allowing industry to leverage the lower cost of cloud services.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
R2.1 is not cost effective as written as it implies all BCSI must be encrypted.	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	No
Document Name	
Comment	
NOT COST EFFECTIVE. There is too much approach-uncertainty and therefore difficult to specifically identify safetly and risk mitigation methods. the proposed updates are adding administrative paperwork which does not improve BES security.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	No

Document Name	
Comment	
The proposed recommendations will provide additional options for protecting BCSI as well as open to more technologies. Additionally, the proposed changes increase the required controls which will reduce risk and increase security. However, these changes are not cost effective and will require investment from entities to implement due to the increased controls and need to protect BCSI throughout the entire lifecycle as well as the increased need to protect BCSI stored in BCS, EACMS, PACS, and PCAs.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy thinks that the proposed recommendations from the SDT would require significant efforts to modify technical, administrative, and operational controls, compliance processes, and evidentiary documentation which carry a high cost and may be ineffective or outdated by the time of implementation.	
Likes 0	
Dislikes 0	
Response	
William Hutchison - Southern Illinois Power Cooperative - 1	
Answer	No
Document Name	
Comment	
Comments: Because of the increases in scope of the standard this could have significant cost increases for REs making using 3rd party storage solutions cost ineffective.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	

Answer	No
Document Name	
Comment	
Not for small entities.	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	

Any changes to Standards with additional obligations does create costs.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Angela Gaines - Portland General Electric Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NextEra	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	

Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	
Document Name	
Comment	
Depends on clarifiaction to question 11.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	

Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
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	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	
Document Name	
Comment	
This cannot be answered until a more thoughtful consideration is given to third-party security objectives.	
Likes 0	
Dislikes 0	
Response	

13. Do you have any other general recommendations/considerations for the drafting team?	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

We feel by including all Medium Impact BES Cyber Systems and eliminating the exclusion of Medium Impact BES Cyber Systems without External Routable Connectivity, this draft of the standard exceeds the scope of the FERC-approved SAR, and does so to no gain while adding significant burden.

The aims of the SAR can be better and more easily achieved by:

1. Defining BCSI Repository

2. Defining BCSI Access

3. Focusing on managing BCSI Access to BCSI Repositories

Likes 0	
Dislikes 0	
Response	

Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	No
Document Name	
Comment	

Support the MRO NSRF comments

Likes 0	
Dislikes 0	
Response	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	

AECI supports comments filed by NRECA	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC agrees with comments submitted by NRECA.	
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	
Thank you for the opportunity to comment.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
In general, PacifiCorp supports EEI and NSRF’s comments proposed for these revisions.	

By eliminating the exclusion of Medium Impact BES Cyber Systems without External Routable Connectivity (ERC), the drafting team is exceeding the FERC SAR.

Many of the proposed changes are not in scope with the SAR and are too prescriptive.

Removing CIP-004 R4.1.3, R4.4, & R5.3 – creates a perceived gap within the access controls designed for CIP-004. We suggest the removal of, “access to BES Cyber System Information (BCSI)”and the replacement with the term “BCSI Respository” or “designated BCSI storage location.” Thusly, termination actions would result in the removal of access to BCSI Repositiories.

If access controls are to be spread throughout the CIP suite of Standards then the references need to be made in both requirements to direct the readers to the correct locations.

CIP-011 R1.1 (A) – Applicable Systems not applicability. Suggested requirement language: Method(s) to identify information that meets the definition of BES Cyber System Information.

CIP-011 R1.1 (B) – Applicable Systems – change to Medium Impact with ERC. Suggested requirement language: Method(s) to identify designated BES Cyber System Information storage locations.

CIP-011 R1.2 - Applicable Systems not applicability. Suggested requiremenet language: Procedure(s) to prevent unauthorized access to BES Cyber System Information during storage, transit, use, and disposal.

CIP-011 R1.3 – Applicable Systems – change to Medium Impact with ERC. Suggested requiremenet language: Process(es) to authorize access to designated BES Cyber System Information storage locations based on need, as determined by the Responsible Entity, except during CIP Exceptional Circumstances.

CIP-011 R1.4 – Remove this requirement and add to CIP-013 where most appropriate.

CIP-011 R1.5 – Applicable Systems – change to Medium Impact with ERC. Suggested requiremenet language: For termination actions, revoke the individual’s current access to designated BES Cyber System Information storage locations, unless already revoked according to CIP-004-7 Requirement R5, Part 5.1) by the end of the next calendar day following the effective date of the termination action.

CIP-011 R1.6 – Applicable Systems – change to Medium Impact with ERC. Suggested requiremenet language: Verify at least once every 15 calendar months that access to designated BES Cyber System Information storage locations, whether physical or electronic, is correct and consists of personnel that the Responsible Entity determine are necessary for performing assigned work functions.

CIP-011 R2 – Suggested language: Each Responsible Entity shall implement one or more documented cryptographic key management program(s) that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Cryptographic Key Management Program.

The draft requirement R2.1 regarding key management is unclear, and yet, at the same time, too prescriptive, with the list of things that should be included. The stated purpose of the SAR is referring to “cryptosystem” key management, but the NERC webinar slide regarding this part listed “physically.”

CIP-011 R2.1 – change Applicability to include “BES Cyber System Information stored in Vendor managed electronic BCSI Repositories”. Suggested requirement language: Where applicable, develop a cryptographic key management process(es) to restrict access with revocation ability, shall include the following: (list of requirement sub parts)

CIP-011 R2.2 – change Applicability to include “BES Cyber System Information stored in Vendor managed electronic BCSI Repositories”. Suggested requirement language: Implement controls to separate the BES Cyber System Information custodial entity’s duties independently from the cryptographic key management program duties established in Part 2.1.

CIP-011 R3 – the requirement is fine as proposed.

Likes 0	
Dislikes 0	

Response

Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC

Answer	No
Document Name	

Comment

NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES

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

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 response found in the NSRF Comment Form

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	

Comment
In general, we support EEI and MRO NSRF comments proposed for these revisions. *By eliminating the exclusion of Medium Impact BES Cyber Systems without External Routable Connectivity (ERC), the drafting team is exceeding the mandate of the SAR.*

Many of the proposed changes are not in scope with the SAR and are too prescriptive.

Removing CIP-004 R4.1.3, R4.4, & R5.3 – creates a perceived gap within the access controls designed for CIP-004. We suggest the removal of, "access to BES Cyber System Information (BCSI)"and the replacement with the term "BCSI Respository" or "designated BCSI storage location." Thusly, termination actions would result in the removal of access to BCSI Repositiories.

If access controls are to be spread throughout the CIP suite of Standards then the references need to be made in both requirements to direct the readers to the correct locations.

CIP-011 R1.1 (A) – Applicable Systems not applicability. Suggested requirement language: Method(s) to identify information that meets the definition of BES Cyber System Information.

CIP-011 R1.1 (B) – Applicable Systems – change to Medium Impact with ERC. Suggested requirement language: "Method(s) to identify designated BES Cyber System Information storage locations [or Repositories]."

CIP-011 R1.2 - Applicable Systems not applicability. Suggested requiremenet language: Procedure(s) to prevent unauthorized BCSI Access during storage, transit, and use.

CIP-011 R1.3 – Applicable Systems – change to Medium Impact with ERC. Suggested requiremenet language: Process(es) to authorize access to designated BES Cyber System Information storage locations based on need, as determined by the Responsible Entity, except during CIP Exceptional Circumstances.

CIP-011 R1.4 – Remove this requirement and add to CIP-013 where most appropriate.

CIP-011 R1.5 – Applicable Systems – change to Medium Impact with ERC. Suggested requiremenet language: For termination actions, revoke the individual's current access to designated BES Cyber System Information storage locations, unless already revoked according to CIP-004-7 Requirement R5, Part 5.1) by the end of the next calendar day following the effective date of the termination action.

CIP-011 R1.6 – Applicable Systems – change to Medium Impact with ERC. Suggested requiremenet language: Verify at least once every 15 calendar months that access to designated BES Cyber System Information storage locations, whether physical or electronic, is correct and consists of personnel that the Responsible Entity determine are necessary for performing assigned work functions.

CIP-011 R2 – Suggested language: Each Responsible Entity shall implement one or more documented cryptographic key management program(s) that collectively include the applicable requirement parts in

CIP-011-3 Table R2 – Cryptographic Key Management Program.

The draft requirement R2.1 regarding key management is unclear, and yet, at the same time, too prescriptive, with the list of things that should be included. The stated purpose of the SAR is referring to "cryptosystem" key management, but the NERC webinar slide regarding this part listed "physically."

CIP-011 R2.1 – change Applicability to include "BES Cyber System Information stored in Vendor managed electronic BCSI Repositories". Suggested requirement language: Where applicable, develop a cryptographic key management process(es) to restrict access with revocation ability, shall include the following: (list of requirement sub parts)

CIP-011 R2.2 – change Applicability to include "BES Cyber System Information stored in Vendor managed electronic BCSI Repositories". Suggested requirement language: Implement controls to separate the BES Cyber System Information custodial entity's duties independently from the cryptographic key management program duties established in Part 2.1.

CIP-011 R3 – the requirement is fine as proposed.

Likes 0	
Dislikes 0	

Response
Ayman Samaan - Edison International - Southern California Edison Company - 1
Answer	No
Document Name	
Comment
Please see comments submitted by Edison Electric Institute
Likes 0	
Dislikes 0	
Response
Wayne Guttormson - SaskPower - 1
Answer	No
Document Name	
Comment
Support MRO comments.
Likes 0	
Dislikes 0	
Response
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1
Answer	No
Document Name	
Comment
In general, we support EEI and MRO NSRF comments proposed for these revisions.
Likes 0	
Dislikes 0	
Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
In general, we support EEI and MRO NSRF comments proposed for these revisions.	
Likes 0	
Dislikes 0	
Response	
William Hutchison - Southern Illinois Power Cooperative - 1	
Answer	No
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	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colleen Campbell - AES - Indianapolis Power and Light Co. - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
While the changes are a good start, significant consideration needs to be performed to consider the various environments the standard will apply to: (1) Information stored by the Entity, which includes many small Entities on both OT and IT systems; (2) Information stored by a Cloud service provider on behalf of an Entity; (3) Information located at a vendor under non-disclosure agreement in active use to meet BES needs.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Small agencies have limited budgets and staff. This approach continues to burden small agencies and we struggle to see any of the proposed changes being cost effective.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	

Answer	Yes
Document Name	

Comment

Duke Energy recommends the following:

- Removing the periodic review requirement in Part 1.4, and allowing the risk assessment to determine necessary reviews and frequency;
- Need more clarity on where or when “factory resets” of a device are sufficient sanitization in reference to Part 3.1;
- R1.2 language is problematic

o Need clarity that we are addressing “unauthorized” ability to obtain

o Eliminate is extremely strong wording

o Likely would require extensive encryption implementation

o Addition of disposal is unclear – do they mean obtaining access after it’s been disposed? Prior to secure disposal;

o Consider the Glossary of Terms used in NERC Reliability Standards: “Operating Plan; Operating Procedure; and Operating Process, for use here and in Part 1.3 rather than “method”, or “process” For greater clarity as to SDT intent.

- R1.3 language is problematic

o How would we authorize access to information in use in a meeting, for example? Are we excpted to keep track of every vendor who has a short term / in-use need to know?

o It would be better to continue focusing authorization for access to storage locations and make that more robust; and

- R1.4 does this presume the Entity has authorized the vendor personnel to access the information (as is typically necessary to store it)? If not, the language is problematic.

o Additionally, do R1.5 and R1.6 apply to these vendor personnel?

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller

Answer	Yes
Document Name	

Comment

Please increase outreach and collaboration using an approach to reach everyone. More than one meeting on specific topic may be needed to reach everyone due to other meeting conflicts and committments. Add written clarity to the Standards so it can stand on its own without needing supporting documents.

A guiodeline WILL be needed. Why not improve the Standard by increasing clarity thereby reducing the need for a Guideline?	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Please provide guidance on the requirements as they relate to encrypting BCSI stored by a Vendor and encrypting BCSI stored on premises.	
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	
We recommend that the scope of the standards team consider leveraging standards such as Fedramp to justify the use of cloud services. We also recommend that the team revist the definition of BES CSI to clear ambiguity. The language and scope of the SAR focused on the resolution of the issue related to the physical control of BES CSI information in transit or use that may not be practical.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Xcel Energy support the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	Yes
Document Name	

Comment

Comments:

-
  - CIP-011-3 R2 Part 2.1 introduces nine terms in its sub-parts 2.1.1 through 2.1.9. These nine terms are not further discussed or defined. While formal Glossary definitions may not be needed, each term should be at least briefly explained. For example, “2.1.1 Key generation – the methods used to create a new encryption key.” Of particular interest is the use of the term “Key suppression.” This term should be clearly explained.
-
  - The SDT should consider the advisability of keeping CIP-011-3’s BES Cyber Asset Reuse and Disposal as Requirement R2 for continuity with CIP-011-2.
-
  - Per CIP-011-3 R3 Part 3.1 that states “Prior to the release for reuse or disposal of applicable Cyber Assets (except for reuse within other systems identified in the “Applicable Systems” column), the Cyber Asset data storage media shall be sanitized or destroyed”, can the referenced Applicable Systems be reused by another entity without adhearing to CIP-011-3 R3 Part 3.1? For example; if parent company A decides to let company B reuse an Applicable System does the company A have to perform its CIP-011-3 R3 Part 3.1 process?
-
  - Is CIP-011-3 R1 Part 1.5 actually feasible for BCSI residing on externally controlled third party systems?

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	Yes
Document Name	2019-02_Unofficial_Comment_Form_201912_MH.docx

Comment

We would suggest making the following changes:

1. Define BCSI Repository (see our definition in Q1)

2. Delete CIP-011-3 R1.3 and R1.5 and make changes in CIP-004-6 (delete existing Part 4.1.3 and Part 4.4) as follows:

See the table provided in response to questions 13 in the attached comment form.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	Yes
Document Name	

Comment

Seattle City Light appreciates the thorough efforts of the 2019-02 Standard Drafting Team to develop more flexible approaches to securing BCSI. We are keenly aware of the many difficulties and pitfalls associated with this endeavor.

Seattle believes, however, that an objective-based approach consistent with and similar to that employed in CIP-013 would provide a more effective solution and avoid the pitfalls and challenges. Specifically, revisions to CIP-004 and CIP-011 might better employ approaches based on a specific security objective (e.g., restrict access of unauthorized individuals to BCSI) and a risk-focused security plan rather than specific controls (control access to BCSI using keys managed by specific practices, etc), combined with requirements for implementation and periodic review. Such an approach achieves the desired security outcome with the double benefit of 1) not precluding use of new technologies outside the control paradigm in use when the Standard was written (as is the case with cloud storage in today's physically-focused Standards) and 2) allowing maximum flexibility to meet the myriad data management methods employed by the hundreds of subject entities across North America.

Likes 0	
Dislikes 0	

Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	

- We believe the SDT went beyond the scope of the SAR. For example, adding a risk assessment similar to CIP-013 was not in scope.
- Suggest making separate requirements for BCSI on premises versus in the cloud.
- Overall it is good to see a futuristic direction with the requirements adapting to technology changes however, some of the changes are too prescriptive and therefore do not encompass current and future capabilities of all technology. Prefer to see goal and objective based requirements, not prescriptive.
- As it relates to Part 1.4, we think there should be a distinction between vendors that are hosting BCSI for the Responsible Entity's use, versus companies that the Responsible Entity provides BCSI to for a project. For example, if the Responsible Entity provides BCSI to a regional entity for an audit, the use and storage of that BCSI by the regional entity should not be in scope of this requirement. Instead, those scenarios should already be addressed by the entity's methods for securing and protecting BCSI.

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	

1) The requirements should be outcome focused and not prescriptive to specific technologies or techniques.

2) The changes to the standard do not provide any clarification regarding the definition of BCSI. This has led to consistency issues across regions regarding what information is considered BCSI. The lack of a clearly understood definition of what comprises BCSI limits the ability to evaluate the security value of the proposed access controls.

Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3	
Answer	Yes
Document Name	
Comment	

AEP is appreciative of the SDT's hard work of developing these proposed modifications. However, we feel that additional revisions are required as shown by our comments. AEP is of the opinion that while on-site storage might be burdensome to some Responsible Entities, BCSI storage on cloud platforms or within third party facilities should be entirely optional. We believe that cloud storage is not a mature enough technology at this time to be able to match the security that on-site storage can provide. AEP also wants to state that given the level of change proposed, we ask that Responsible Entities be provided with more time to ensure compliance by pushing the enforcement deadline to a later date.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	Yes
Document Name	

Comment

NRECA believes the removal of requirements form CIP-004-6 to CIP-011-3 was not authorized by the SAR for this project. In particular, the SAR explicitly stated that CIP-004 be modified and that CIP-011 be evaluated for any downstream type impacts. It did not authorize the wholesale removal of requirements from CIP-004-6. Accordingly, the SDT revisions go beyond the scope of the SAR as provided below:

CIP-004-6 Requirements need to be modified so management of access to BCSI is clarified to include a focus on the BCSI data and the controls deployed to limit access. In addition, the Standard should allow various methods for controlling access to BES Cyber System Information, storage location(s). … In addition to CIP-004-6 modifications, CIP-011-2 should also be evaluated for any subsequent impacts.

NRECA recommends that NERC develop a process to gain industry consensus on proposed changes to CIP standards prior to the formation of a standards drafting team for modifications that are not directed by FERC. Multiple standards drafting teams have spent significant time attempting to make modifications to the standards for which there is no industry consensus that the modification is needed. This places the Standard Drafting Team in an untenable position and consumes a substantial amount of industry resources without benefitting reliability or security.

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

Many of the proposed changes are not in scope with the SAR, are too prescriptive, and cause confusion rather than provide clarification. We don't believe the current standards, as written, preclude the use of cloud storage vendors and encryption technologies. In light of the fact that the CMEP

Guidance came out after the SAR, we wonder if changing the standards is needed. If needed, any further clarification can be done via additional guidance.

We disagree with the change in R1, Part 1.1 from “Method(s)” to identify information” to “Process(es) to identify information.” This would cause programs which use a method to identify information to be non-compliant. The last example of evidence is one such method--One can know that something is BCSI (identify it) just by the fact that it is in a specified location or repository. Technical Rationale for CIP-011-2, Requirement 1, paragraph 4 states: *“The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity’s program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of* ***methods that the entity may choose to utilize for the identification of BES Cyber System Information****.”* [emphasis added] Measure could be re-written as such: Documentation that information stored in a specified location is considered BCSI.

We disagree with having requirements for disposal in two different parts (R1 Part 1.2 and R3 Part 3.1) as this could result in double jeopardy during audits as auditors review disposal procedures for compliance with R1 and then again with R3. This change exceeds the SAR, and R3 takes the focus off protecting the information (BCSI), which has always been the intent of this part and CIP-011 as a whole. R3 also brings all Cyber Assets into scope, not just those that contain BCSI. We propose removing disposal from R1 Part 1.2 and reverting back to the CIP-011-2 version of R2 asset reuse and disposal as separate requirements.

We do not see how chain of custody is a measure of sanitization or destruction. In addition, this term was rejected by commenters and the SDT of a prior version of the standard.

The proposed High VSL is not appropriate or in line with other standards. As it reads, any instance of unauthorized access automatically results in a High VSL. A breach is always possible even with a sound plan and implementation. We propose removing the additional High VSL altogether, or looking to other standards which base VSL on included parts of the plan, or number of instances.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	

GSOC respectfully suggests that the removal of requirements form CIP-004-6 to CIP-011-3 was not authorized by the SAR for this project. In particular, the SAR explicitly stated that CIP-004 be modified and that CIP-011 be evaluated for any downstream type impacts. It did not authorize the wholesale removal of requirements from CIP-004-6. Accordingly, the SDT revisions go beyond the scope of the SAR as provided below:

CIP-004-6 Requirements need to be modified so management of access to BCSI is clarified to include a focus on the BCSI data and the controls deployed to limit access. In addition, the Standard should allow various methods for controlling access to BES Cyber System Information, storage location(s). … In addition to CIP-004-6 modifications, CIP-011-2 should also be evaluated for any subsequent impacts.

GSOC recommends that NERC develop a process to gain industry consensus on proposed changes to CIP standards prior to the formation of a standards drafting team for modifications that are not directed by FERC. Multiple standards drafting teams have spent significant time attempting to make modifications to the standards for which there is no industry consensus that the modification is needed. This places the Standard Drafting Team in an untenable position and consumes a substantial amount of industry resources without benefitting reliability or security.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

We have concerns with the Measures in Part 3.1 on “chain of custody” as too prescriptive
We have concerns with Part 3.1 on demonstrating compliance with a) destruction of virtualized equipment and b) re-deployment of virtualized assets

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper

Answer	Yes
Document Name	

Comment

We recommend the SDT consider development of a standard just for cloud services. This will eliminate confusion and ambuiguity for the current standards.

Likes 0	
Dislikes 0	

Response

Vivian Moser - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	

Comment
AZPS considers the proposed CIP-011-3 to exceed the scope of the SAR; however, recognizes the intent to increase the security posture for BCSI. For this reason, AZPS offers the following recommendations for the SDT's consideration: • Revise the proposed language to better delineate between protection of BCSI in use, transit, and disposal, and access to BCSI storage locations. • Revise the applicability language to clearly establish focus on BCSI. As provided in our response to Question No. 5, AZPS offers the following suggested wording: "System information pertaining to (but not including the BES Cyber System (BCS) which may contain BCSI):…" • Reconsider the addition of CIP-011-3 R2 as currently drafted. AZPS asserts that requiring a key management program is overly prescriptive (see further comments on this requirement included in the AZPS response to Question No. 8).

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	

Comment
Several of the proposed revisions are outside of the SAR, and this draft is too prescriptive and absolute in its language, and therefore not risk-based nor technology agnostic. Additionally, within this comment form, the SDT did not seek feedback on the proposed language in Part 3.1. This proposed language is a step backwards and posed undue administrative burden without a commensurate security or reliability benefit. The requirements should be focused on security and reliability value, and sanitization or destruction of data storage media not containing BCSI does not provide security nor reliability value. In fact, for entities that may have life cycle processes in place to reuse equipment in a less critical capacity after a refresh in the critical environment (perhaps test or dev, as one example) the requirement as written precludes an entity from reusing a non-BCSI device with a known and standardized OS configuration, patch level, etc. in a different capacity outside the environment without a full sanitization and rebuild. This is an inefficient use of Registered Entity's limited resources.

Likes 0	
Dislikes 0	

Response

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3	
Answer	Yes
Document Name	
Comment	
We believe the SDT went beyond the scope of the SAR. For example, adding a risk assessment similar to CIP-013 was not in scope. Suggest making separate requirements for BCSI on premises versus in the cloud. Overall it is good to see a futuristic direction with the requirements adapting to technology changes however, some of the changes are too prescriptive and therefore do not encompass current and future capabilities of all technology. Prefer to see goal and objective based requirements, not prescriptive. As it relates to Part 1.4, we think there should be a distinction between vendors that are hosting BCSI for the Responsible Entity's use, versus companies that the Responsible Entity provides BCSI to for a project. For example, if the Responsible Entity provides BCSI to a regional entity for an audit, the use and storage of that BCSI by the regional entity should not be in scope of this requirement. Instead, those scenarios should already be addressed by the entity's methods for securing and protecting BCSI.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	Yes
Document Name	NRECA comments 2019-02_Unofficial_Comment_Form_201912 (1) 013120.docx
Comment	
See NRECA submitted comments.	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	

In order to properly shift the approach of information protection to focus on the information and not the storage locations, the requirement for declaration of storage locations must be either removed or eased to focus on information residing with a vendor or third-party provider (e.g. cloud.) In addition, information residing within a BCS environment should be fully exempt from this requirement as the existing CIP-004, CIP-005, and CIP-006 protections will protect the information as long as it does not leave the BCS environment.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	Yes
Document Name	

Comment

(1) N&ST recommends retaining the existing language of CIP-011-2 Requirement R1, Part 1.2 (“Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.”) In addition to objecting to the proposed “obtain and use” language in a revised Part 1.2, N&ST notes that as written and if interpreted literally, the proposed requirement would compel a Responsible Entity to ensure that NOBODY could “obtain and use” BCSI.

(2) While N&ST opposes moving existing BCSI storage location access management requirements from CIP-004 to CIP-011, we support the SDT’s proposals to modify CIP-011’s “Applicability” column entries and to add an explicit requirement to identify BCSI storage locations. N&ST believes that if this is done, the “Applicability” of CIP-004 requirements that apply to BCSI storage locations (R4 Part 4.1.3, R4 Part 4.4, and R5 Part 5.3) should be changed to “Identified BCSI Storage Locations.” N&ST understands this change would likely compel moving R4 Part 4.1.3 to a revised R4 Part 4.2 and renumbering existing R4 Parts 4.2 – 4.4 to R4 Parts 4.3 – 4.5.

Likes 0	
Dislikes 0	

Response

ALAN ADAMSON - New York State Reliability Council - 10

Answer	Yes
Document Name	

Comment

The NYSRC is casting NEGATIVE vote because of these concerns:

• We have a concern regarding Requirement 1.4, which calls for risk identification, assessment, and mitigation for entities choosing to use a vendor to manage their BCSI. The risk identification and assessment portion of the requirement overlaps with CIP-013. We would like to know why the SDT is requiring mitigation for CIP-011 compliance when it is not required for CIP-013 compliance. Also, this Requirement calls for a re-assessment at

least once every 15 months. We believe that the value that this would add to cybersecurity programs may be outweighed by the cost of performing the reassessment (and subsequent mitigation).

• There is ambiguity vis-à-vis the data destruction requirement for High & Medium Impact BES Cyber Systems. Does this apply to virtualized BES Cyber Assets? What about BES Cyber Assets with read-only memory?

• Requirement 2.2 – separation of duties between BCSI custodian and key-management custodian – will be difficult to implement for entities that use physical keys, since in those instances it will most likely be the same individual(s) responsible for both sets of duties.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Dominion Energy supports EEIs comments.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	Yes
Document Name	

Comment

Ameren agrees with and supports EEI comments.

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

CIP-011 R3 has increased in scope from BES Cyber Assets that may contain BCSI to the sanitization or destruction of ALL data storage media for ALL BES Cyber Assets. This language removes from the Responsible Entity the ability to determine *if* a BES Cyber Asset contains BCSI, and if so, take measures to prevent the unauthorized retrieval of said BCSI, and in turn requires the sanitization or destruction of ALL BES Cyber Assets. What purpose is served by sanitizing or destroying an asset that does not contain BCSI? There is no rationale for this change documented in the Technical Rationale document. We believe this requirement to now be problematic as there may be BES Cyber Assets that are firmware based and thus have "data storage media" for their firmware code but have no capability to store BCSI. They are now in scope of this requirement, however there is no need (and may have no ability) to wipe their firmware code. This requirement then forces the destruction of those devices that cannot be sanitized but that do not contain BCSI, and this is an undue burden placed upon entities with **no** security benefit.

We also find that CIP-011 R3 is the one requirement that was explicitly hardware based, and it retains its hardware basis even though Question 9 implies that enabling cloud solutions would require the move away from hardware basis. The suggested change also presents issues with today's on-premise virtualized environments where a virtual BES Cyber Asset with virtual storage, the virtual storage may be destroyed but that is not technically the "data storage media". The entity may not be able to map a logical, virtual storage unit to the actual "storage media" in the underlay on which the data resided, and it cannot wipe or destroy physical media without impacting other live BES Cyber Assets.

We suggest the requirement simply state:

"Prior to the release for reuse or disposal of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of the BES Cyber System Information."

There should be a clear delineation between Affiliate Restrictions requirements (the Standards of Conduct) for protecting information which may include BCSI and the R1 Requirement of "Process to identify information that meets the definition of BES Cyber System Information…"

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	Yes
Document Name	

Comment

We have concerns with the Measures in Part 3.1 on "chain of custody" as too prescriptive.

We have concerns with Part 3.1 on demonstrating compliance with a) destruction of virtualized equipment and b) re-deployment of virtualized assets.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	Yes
Document Name	

Comment

The effort put forth by the SDT is appreciated. However, we encourage the SDT to review the approved SAR and focus on adding requirements that meet the objective of clarifying protections for cloud-based service providers, while keeping the burden on entities that do not use cloud-based providers to a minimum. Additionally, while adding clarity around managing access to BCSI and securing BCSI, the SDT should consider how the changes might impact or be similar to other requirements and attempt to avoid instances of added confusion or spaghetti requirements (access management and vendor risk management). As stated in other drafting teams, the industry is looking for risk-based requirements, and adding more specificity to requirements defeats this concept.

Furthermore, there were no questions specific to the implementation plan, but as proposed today, 18 months does not seem sufficient. As discussed above, adding Medium Impact and PCAs could take significant time to implement across a large number of new assets, locations and information. Additionally, the vendor risk assessment could cause entities to modify their vendor agreements, which in turn could increase costs to the entities.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2

Answer	Yes
Document Name	

Comment

Yes – MISO commends the SDT for its efforts to consolidate like requirements and suggest the existing standards evolve to align with industry security standards, such as NIST 800-53 and ISO 27001.

In addition, MISO recommends that each requirement be reviewed and restated as applicable to focus on results; i.e. the protection of BES Cyber Security Information : prevent unauthorized access to BCSI (performance-based), perform testing/simulations that demonstrate inability to access BCSI without authorization (risk-based) and document procedures to prevent unauthorized access to BCSI (competency-based). Monitor performance via periodic reporting of test/simulation results, actual security breaches/events, other?

Finally, MISO proposes the issue of electronic disposal be addressed. MISO suggests the SDT consider updating CIP-011-3, requirement R3 to provide objective based requirements related to disposal. As written, the standard would be administratively burdensome from an evidence perspective.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Although EEI recognizes and appreciates the work done by the SDT to enhance entity options as it relates to the use of cloud-based services for the storage of BCSI, many of the proposed changes are not in the scope of the approved SAR and are too rigid. The SAR seeks clarifying language that would allow entities to safely and securely store BCSI on third-party cloud-based services. Thus, the change could be made through minor modifications, such as developing new definitions (i.e., “BCSI Repository” and “Useable Access”) along with a few minor changes as suggested in our response to question 4 (above). In addition, adding vendor assessment requirements into CIP-011, while also moving requirements from CIP-004 to CIP-011, seem to conflict with one another. To the extent the SDT is concerned about potential reliability gaps meriting the proposed changes, a new SAR should be developed with technical justification. EEI also notes that the SDT did not ask about the appropriateness of the Implementation Plan. Given the level of change proposed, specifically related to vendor contracts, entities will need at least 24 months to achieve compliance with these new requirements.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Language in part 1.2 does not align with the language in part 1.5, requiring a method to eliminate ability to obtain and use BCSI in one and revoke individual’s access to BCSI in the other. This language mismatch will lead to confusion. Also, sub-requirement 2.1.2 is missing.	

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2

Answer	Yes
Document Name	

Comment

NYISO commends the SDT for its efforts to consolidate like requirements and suggest the existing standards evolve to align with industry security standards, such as NIST 800-53 and ISO 27001.

In addition, NYISO recommends that each requirement be reviewed and restated as applicable to focus more on results and security objectives; i.e. the protection of BES Cyber Security Information : prevent unauthorized access to BCSI (performance-based), perform testing/simulations that demonstrate inability to access BCSI without authorization (risk-based) and document procedures to prevent unauthorized access to BCSI (competency-based).

Further improvements of the draft should consider:

- Separate and keep access authorization and revocation centrally maintained as part of CIP-004. Adding a reference to the CIP-004 requirements from within CIP-011. The related CIP-004 requirements should also be reviewed and updated.

- Clarify that Responsible Entities should determine protective measures for BCSI based on risk and that solution measures other than encryption may be acceptable.

- Keep together those requirements related to BCSI stored in environments owned by third parties (and in a way, that is not redundant).

- Clarify that vendor risk assessment requirement can be accomplished via CIP-013 SCRM program

- Adding clarification on the term, “obtain.” Would like assurance that we have a consistent understanding of what is meant between “Obtain and Use” versus “Obtain or Use.”

- NYISO agrees that all risk assessments requirements should be housed within CIP-013 and would suggest further clarification as to what type of vendor needs to be risk assessed dependent on the type of cloud service is being procured and used (e.g. IaaS, Paas

- All access should be revoked within the specified period for any reason where an individual no longer requires it, not just termination.

- NYISO definitely sees the benefit in key management conceptually, but the language is too ambiguous and confusing therefore, we cannot endorse it.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NextEra

Answer	Yes

Document Name	
Comment	
1) We have concerns with the Measures in Part 3.1 on “chain of custody” as too prescriptive. 2) We have concerns with Part 3.1 on demonstrating compliance with a) destruction of virtualized equipment and b) re-deployment of virtualized assets.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Could there be a standard in providing some form of industry threshold qualifications to vendors to reduce the responsibility and remove the onus of entities subject to reliability standards to perform Vendor risks assessments and establish controls to mitigate these risks. Current model puts all pressures on entities to conduct all work on BCSI risk. Possibility to look at NIST / FedRAMP standards. Also please consider in providing additional guidelines on what constitutes "BCSI".	
Likes 1	BC Hydro and Power Authority, 5, Hamilton Harding Helen
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	Yes
Document Name	
Comment	
We have concerns with the Measures in Part 3.1 on “chain of custody” as too prescriptive We have concerns with Part 3.1 on demonstrating compliance with a) destruction of virtualized equipment and b) re-deployment of virtualized assets.	
Likes 0	
Dislikes 0	
Response	

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	
Please review the proposed language with an eye toward increasing the use of narrow scope. Explicit, and affirmative language is necessary to eliminate ambiguity and inspire confidence in not running afoul of compliance should an entity choose to store BCSI in the cloud. There should be no confusion as to what is and what is not permitted. Please investigate establishing reciprocity for Federal IT certifications.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Consider encompassing access management within one holistic Standard. The departure and movement of access management requirements amongst several Standards seem to be a step backwards from security integration and collaboration between programs.	
Likes 0	
Dislikes 0	
Response	

James Brown - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	

- Overall, it appears that this version of requirements, specifically R.1.4, is intended to address situations where a Responsible Entity contracts with another party for the storage and processing of BCSI. With that intention, measures on each requirement would benefit from adding specific ways to demonstrate compliance when using a third party.
- Requirement R1.4 does not include minimum security requirements the risk assessments of vendors need to include, such as security training, access controls, and termination actions. A minimum set of expectations should be defined.
- Any requirements allowing the use of third party provider should also include measures on the use of external audits performed by accredited auditors (e.g. SOC) in demonstrating compliance with the requirement. This would include all access management and data destruction requirements.
- Can the drafting team provide more detail on the distinction between “data” about BES Cyber Systems and “information” about BES Cyber Systems? Although the distinction is made in the definition, the distinction is not addressed in requirements or measures. Usability of the information is the key.
- Part 1.3 should be moved to CIP-004 with the proposed language.
- Part 1.5 should be moved to CIP-004 with the proposed language.
- Requirement Part 2.2 should note that separation of duties is only necessary when a vendor or other third-party is housing the information. This should not be required if the information is stored on-premises with the Responsible Entity.
- Requirement Part 3.1 is redundant to Part 1.2.
- As the drafting team is considering updating the standards, suggest the existing standards evolve to align with industry security standards, such as NIST 800-53 / ISO 27001, and be more objective and outcome based changes.
- In reviewing this, it appears that the definition of BCSI should be modified to remove the examples. The definition allows for a risk-based approach to identifying BCSI but the examples are being used as an authoritative list and not as a form guidance. The examples should be removed from the definition and guidance written through other means.
- There appears to be no actual requirement for security awareness training for individuals with access to BCSI. CIP-011-3, R1.1, lists “training materials that provide personal with sufficient knowledge to recognize BCSI” as an example, not a requirement, of acceptable evidence. CIP-004-7, R2.1.5 requires training content on “Handling of BES Cyber System Information and its storage”, but this is applicable only to individuals with access to High and Medium Impact BES Cyber Systems~. This needs to be clarified to prevent a difference in interpretation between the Responsible Entity and the Auditor. Is has been noted that there is no requirement to perform Personnel Risk Assessments on individuals with access to BCSI.

Likes 0	
Dislikes 0	
Response	

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG is in agreement with RSC provided comment	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	Yes
Document Name	
Comment	
PGE agrees with EEI's general recommendations, particularly that the SDT could pursue minor modifications, such as new definitions, to achieve the SAR's objective.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Without splitting EACMS into EACS and EAMS the issue of third-party analysis systems is not addressed but is included in the SAR. Please ensure that EACMS is split into EACS and EAMS in order to address this issue. Third-party analysis systems currently are include in the EACMS definition, splitting the definition would allow EAMS to be applicable within only the CIP-011 standard, and simplify use of these third-party services.	
Likes 0	
Dislikes 0	
Response	

Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	

We have concerns with the Measures in Part 3.1 on “chain of custody” as too prescriptive. We have concerns with Part 3.1 on demonstrating compliance with a) destruction of virtualized equipment and b) re-deployment of virtualized assets.

Likes 0	
Dislikes 0	
Response	

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

ERCOT offers the following additional comments:

- Overall, it appears that this version of the requirements, specifically Part 1.4, is intended to address situations where a Responsible Entity contracts with another party for the storage and processing of BCSI. ERCOT believes there is benefit to including measures on each requirement that identify specific ways to demonstrate compliance when using a third party.
- Part 1.4 does not include minimum security requirements the risk assessments of vendors need to include, such as security training, access controls, and termination actions. ERCOT believes a minimum set of expectations should be defined.
- ERCOT believes that any requirements allowing the use of third party providers should also include measures on the use of external audits performed by accredited auditors (e.g. SOC) in demonstrating compliance with the requirement. This would include all access management and data destruction requirements.
- Is the drafting team able to provide more detail on the distinction between “data” about BES Cyber Systems and “information” about BES Cyber Systems? Although the distinction is made in the definition, the distinction is not addressed in requirements or measures. ERCOT believes usability of the information is the key.
- ERCOT suggests Part 1.3 should be moved to CIP-004 with the proposed language.
- ERCOT suggests Part 1.5 should be moved to CIP-004 with the proposed language.
- ERCOT suggests Part 2.2 should note that separation of duties is only necessary when a vendor or other third-party is housing the information. This should not be required if the information is stored on-premises with the Responsible Entity.

- Part 3.1 is redundant to Part 1.2.
- As the drafting team is considering updating the standards, ERCOT suggests the existing standards evolve to align with industry security standards, such as NIST 800-53 / ISO 27001, and be more objective and outcome based.
- ERCOT suggests that the definition of BCSI should be modified to remove the examples. The definition allows for a risk-based approach to identifying BCSI, but the examples are being used as an authoritative list instead of a form of guidance. ERCOT believes the examples should be removed from the definition, and guidance written through other means.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL

Answer	Yes
Document Name	

Comment

Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: James Mearns, 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 recommends the SDT consider including the ability for an entity to use industry or federally approved certifications such as FedRAMP for CIP-011 R1, Part 1.4 in place of doing their own risk assessment.

Likes 0	
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Comments: ISO-NE commends the SDT for taking on the challenge to address BCSI compliance issues that existed even in the CIPv3 days. ISO-NE recommends that the SDT consider approaching the information security risks and protections on an objective basis instead of a prescriptive basis. The standard should require the parts/elements/criteria that must be included in a security risk assessment plan without prescribing solutions or technologies. As stated in the SAR, the standard should allow multiple methods for controlling access to BES Cyber System Information.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Angela Gaines - Portland General Electric Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Russel Mountjoy - Midwest Reliability Organization - 10	
Answer	
Document Name	
Comment	
MRO appreciates the efforts of the 2019-02 team over the past months. While there is good in the draft, the proposed language for CIP-011-3 Part 1.4 is too high level. Requiring a "Process to identify, assess, and mitigate risks…" offers no direction as to what risk considerations are a concern. *As discovered by the 2016-02 CIP SDT, objective based requirements seem to hit the mark when the requirement language guides the 'what', but not the 'how'. If 'mitigate the risk' language is used, the language should guide entities to address a minimum set of risk considerations. Risk considerations should include risk categories that are typical for the cloud environment, such as service level agreements, encryption (logical protections), data sovereignty, data transformations, and certifications.* *If left as written, the ERO enforcement of this objective based requirement will likely become equally open ended.*	
Likes 0	
Dislikes 0	
Response	

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	
Document Name	
Comment	
CIP-011-3 R1.6. - Suggest a rewording of the requirement to "Verify at least once every 15 calendar months that access to BES Cyber System Information is correct and that the Responsible Entityt determines is necessary for performing assigned work functions." CIP-011-3 R3.1 - This requirement is not needed if the term 'sanitization' is included in Part 1.2 as discussed in Q4. Any associated measures could be included there as well.	

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE has the following additional comments: • Part 3.1 table header: should be revised from “BES Cyber Asset Reuse and Disposal” to “Cyber Asset Reuse and Disposal”, the applicable systems column contains EACMS, PACS, and PCAs as well. • Update the Applicable Systems columns in CIP-004-7 R4 (Parts 4.1-4.3) and R5 (Parts 5.1-5.4), to include PCA and Medium Impact BES Cyber Systems (versus Medium Impact BES Cyber Systems with External Routable Connectivity). Since CIP-011-3 Part 3.1 includes EACMS, PACS, and PCA, this change would align better CIP-004-7 better with CIP-011-3 as well as improve an overall security posture for access management and revocation.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
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	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	
Document Name	
Comment	
The standards development team should draft separate requirements for cloud vs in house BCSI.	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	
Document Name	
Comment	

See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	