NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	Project 2019-02 BES Cyber System Information Access Management
Comment Period Start Date:	3/28/2019
Comment Period End Date:	4/26/2019
Associated Ballots:	

There were 47 sets of responses, including comments from approximately 121 different people from approximately 93 companies representing 10 of the Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Vice President of Engineering and Standards, Howard Gugel (via email) or at (404) 446-9693.

Questions

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

2. Provide any additional comments for the SAR drafting team to consider, if desired.

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities

10 — Regional Reliability Organizations, Regional Entities

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
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
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
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administration	1,6	MRO

					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Brad Parret	Minnesota Powert	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service Corporation	3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent ISO	2	MRO
Westar Energy	Douglas Webb	1,3,5,6	MRO,SPP RE	Westar-KCPL	Doug Webb	Westar	1,3,5,6	MRO
					Doug Webb	KCP&L	1,3,5,6	MRO
ACES Power Marketing	Jodirah Green	1,3,4,5,6			Bob Solomon	Hoosier Energy Rural	1	SERC

			MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations		Electric Cooperative, Inc.		
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Ginger Mercier	Prairie Power , Inc.	1,3	SERC
					Susan Sosbe	Wabash Valley Power Association	3	SERC
					Jennifer Brey	Arizona Electric Power Cooperative, Inc.	1	WECC
					Bill Hutchison	Southern Illinois Power Cooperative	1	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
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,RF,SERC	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Lee Schuster	Duke Energy	3	FRCC

					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Manitoba Hydro	Mike Smith	1,3,5,6		Manitoba Hydro	Yuguang Xiao	Manitoba Hydro	5	MRO
					Karim Abdel-Hadi	Manitoba Hydro	3	MRO
					Blair Mukanik	Manitoba Hydro	6	MRO
					Mike Smith	Manitoba Hydro	1	MRO
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC

Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion	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
					Michael Jones	National Grid	3	NPCC
					Sean Cavote	PSEG	4	NPCC

Kathleen Goodman	ISO-NE	2	NPCC
David Kiguel	Independent	NA - Not Applicable	NPCC
Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
Gregory Campoli	New York Independent System Operator	2	NPCC
Caroline Dupuis	Hydro Quebec	1	NPCC
Chantal Mazza	Hydro Quebec	2	NPCC
Laura McLeod	NB Power Corporation	5	NPCC
Nick Kowalczyk	Orange and Rockland	1	NPCC
John Hastings	National Grid	1	NPCC
Joel Charlebois	AESI - Acumen Engineered Solutions	5	NPCC

	International Inc.		
Quintin Lee	Eversource Energy	1	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
Michael Forte	Con Ed - Consolidated Edison	1	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

Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		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
PSEG	Sean Cavote	1,3,5,6	FRCC,NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	NPCC
					Karla Barton	PSEG - PSEG Energy Resources and Trade LLC	6	RF
					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co.	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co.	1	RF

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	

Reclamation agrees that a cost-effective, risk-based approach for the adoption and use of cloud services is needed within industry. BES Cyber System Information could be stored on third party systems if proper controls for confidentiality, integrity, and availability are implemented for acceptable risk to the BES. For example, if BCSI is stored within a cloud server and encrypted, the entity that owns the data should be the only one with access to the encryption keys capable of decrypting the data, availability during critical emergencies, and integrity of transport layers 2 and 3.

Reclamation disagrees with the statement, “As currently drafted, the requirement is focused on access to the ‘storage location,’ and therefore does not permit methods such as encryption and key management to be utilized in lieu of physical/electronic access controls. This wording also does not explicitly permit any flexibility in the audit approach.” The current CIP-004 standard does not exclude these methods.

Virtualization can and should be as simple as, “If it is something that needs to be protected, protect it.” Reclamation recommends registered entities be allowed to determine their risks. Reclamation is concerned that the proposed requirements will lead to increased requirements for low impact systems. The SDT must consider allocation of resources spent on managing and documenting efforts on low impact systems. The SAR seems to indicate that everyone would need specific authorization versus the current method of allowing a position of authority to delegate who may have access. More detailed categorization will require more tracking tools and create more opportunities for failure (non-compliance) without necessarily improving BES reliability or reducing risk.

Reclamation recommends the SDT focus on defining what BCSI is; specifically, if it is information carried **through** the BES Cyber System or **about** the BES Cyber System.

Likes 1	Minnkota Power Cooperative Inc., NA - Not Applicable, Fuhrman Andy

Dislikes 0	
Response	
Thank you for your comment. The SAR DT has revised the SAR to more accurately state what the SDT would be addressing with the future proposed revisions. The scope of the proposed SAR is only related to High and Medium Impact BES Cyber Systems. The consideration of the definition is included in the scope of the SAR.	
Oliver Burke - Entergy - Entergy Services, Inc. - 1	
Answer	No
Document Name	
Comment	
The goal of restricting access to BCSI to only authorized personnel is to ensure the confidentiality, integrity, and availability of the data. Entities need to have flexibility of defining how this is accomplished. Limiting entities to specific requirements and technology hinders a company's ability to use tools that may protect them more effectively. A good example of this problem involves access revocation requirements for BCSI. Currently we must revoke access within the next business day. Certainly, a revocation process is necessary, but a specific time frame makes it almost impossible to manage service solutions such as cloud services. The regulatory controls that govern BCSI should guide entities to build strong risk-based data protection plans for their BCSI, not limit them to specific technologies or measures. Doing this restricts their ability to implement modern security programs and best-of-breed tools based on current and evolving threat landscapes. While this SAR doe mention specific technologies that could assist in preventing unauthorized access to BCSI, we are concerned that it will provide only minimal expansion of what is acceptable rather than giving each entity the flexibility it needs.	
Likes 1	Minnkota Power Cooperative Inc., NA - Not Applicable, Fuhrman Andy
Dislikes 0	
Response	

Thank you for your comment. The Requirements concerning access management and the flexibility are included in the scope of the revised SAR.	
Shari Heino - Brazos Electric Power Cooperative, Inc. - 1,5	
Answer	No
Document Name	
Comment	
We do not believe that the standards require revision in order to accommodate cloud storage, encryption, or various other tools which may be used for protection of BCSI. CIP-004-6 is written to accommodate a variety of vetting and authorization approaches. For BSCI access under CIP-004, R4.1 merely specifies that a Responsible Entity must have a *process* to "*authorize based on need, as determined by the Responsible Entity*," for the types of access listed in 4.1.1 through 4.1.3. This provision does not specify a requirement to do background or identity checks on individual third party employees. It does not preclude the ability of a Responsible Entity to use a cloud provider to store BSCI; it merely requires codifying and implementing an approach to authorizing access to BCSI storage, if actual access will even occur. Terms such as "access," "designated storage location," and "termination action" are undefined in the standards, and, depending how defined in the Responsible Entity's process, could allow third party cloud storage of BSCI while still meeting the current standards. If the drafting team determines that changes should be made; however, we recommend that, (1) such changes should be clearly couched as clarifications, and (2) highly specific or qualitative requirements regarding cloud storage and encryption should be avoided. Technology and cyber attacks are changing daily, and our requirements should remain flexible regarding the protections we choose to use.	
Likes 1	Minnkota Power Cooperative Inc., NA - Not Applicable, Fuhrman Andy
Dislikes 0	
Response	
Thank you for your comment. The Requirements concerning access management and the flexibility are included in the scope of the revised SAR.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No

Document Name	
Comment	

While Dominion Energy supports cloud computing, Dominion Energy does not support the instant SAR. In stating the industry needs to allow BCSI data to be stored on the cloud using encryption rather than the current requirements of the CIP standards, the SAR does NOT present a reliability purpose to allow this less stringent method of storage of BCSI data. The need statement actually appears to potentially create a reliability gap by asserting that encryption alone could be an alternative to the existing requirements. The SAR is proposing to use specific technologies (i.e. encryption and key management) which could be less secure when used as an alternative to current CIP requirements.

Dominion Energy is also of the opinion that the SAR is requesting a modification solely for compliance clarification. A standard modification may not be the appropriate tool, rather Implementation Guidance should be used to clarify compliance expectation. The current requirements do not need to be modified to allow cloud storage of information and is appropriate based on the nature of the information being protected (BCSI). Dominion Energy is of the opinion that the term 'access', which is a key issue in the SAR, standard could be defined as "the ability to use" when used in the context of electronic access; therefore, a change to the standard wouldn't be necessary to allow an entity to take credit for controls that prevent access; such as, encryption and key management as methods for controlling physical/electronic access.

As an example, if an individual can log into a server that contains an electronic storage location but doesn't have the ability to use the data because the individual doesn't the rights to access the data, there's no compliance issue because the individual doesn't have the ability to use the data.

The issue statement for cloud computing is ensuring the entity has an ability to know who has access to the BCSI information. o Given the nature of the environment, it may not be clear who (outside of the entity) has access to the designated electronic storage location.

There may also be supply chain implications to be able to contractually ensure an entity is able to ensure administrators of the cloud computing vendor are not provisioned in such a way that they would ever have unauthorized access to a designated BCSI storage repository.

From a cyber-security perspective, use of cloud computing for confidential information increases the risk of information falling into the hands of a 'bad actor':

An entity loses control of the data as soon as it's in the cloud. This includes not only the storage location but the transport from the source to the third-party storage location.

Even though the BCSI may be may be encrypted, there's no assurance that a copy of the encrypted data can't be made. A copy of the encrypted data can be held by "bad actors" until such time as the technology exists to break the encryption.

It may not be clear who administratively has access to the electronic storage location from the cloud storage vendor.

The cloud storage vendor may subcontract portions of the administration of the environment.

There is no assurance that confidential files will be properly destroyed once it's determined they're no longer needed.

Due to the nature of cloud storage, multiple copies of a designated storage location may exist for redundancy in strategically placed data centers. Deleting a repository in one data center doesn't mean all copies (and backup copies) are also deleted.

For these reasons, Dominion Energy does not support this SAR and recommends that an Implementation Guidance document, which is appropriate to address the compliance concerns raised in the SAR, be explored.

Likes 1	SCANA - South Carolina Electric and Gas Co., 1,3,5,6, Shumpert RoLynda
Dislikes 0	

Response

Thank you for your comment. The SAR DT asserts that revisions to the current standards are needed to provide further clarity.

Andy Fuhrman - Minnkota Power Cooperative Inc. - NA - Not Applicable - MRO

Answer	No
Document Name	

Comment

MPC agrees that CIP-004 can be updated to better accommodate cloud-based storage, however, the current scope misses out on opportunites to align CIP-004 with the risk-based approach of CIP-012 and CIP-013. CIP-011 is currently risk based, but the examples provided in the SAR

are highly prescriptive and should be considered a step backwards. The scope of this project should accommodate cloud storage by echoing CIP-012 R1 language, such as: *"The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure of BCSI. This shall be accomplished by one or more of the following means, to include BCSI that is in storage, transit, and use:* • *Encryption and key management;* • *Physical access management;* • *Electronic access management;* • *Data loss prevention techniques and rights management services; or* • *Using an equally effective method to mitigate the risk of unauthorized disclosure."* *The scope of this project needs to include authorization and access restrictions to BCSI, not to a "designated storage location".*

Likes 0	
Dislikes 0	

Response
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	

Comment
Dominion Energy South Carolina (formerly SCANA) is in agreement with comments submitted by Dominion Energy (Sean Bodkin).

Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see response to Dominion Energy.	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Electric Reliability Council of Texas, Inc. (ERCOT) requests that the SAR expressly identify the option of creating a separate standard for solutions involving third-parties rather than embedding new requirements in existing requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	

Thank you for your participation.	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Permitting methods such as encryption and key management to be utilized to as an additional protection for BCSI in transit and use allows improvements to the standard for CIP-011-2. However, cloud services are of a concern to the security of storing and allow multiple methods for controlling access to the BES Cyber System Information storage location may pose additional risks.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
GSOC supports the proposed scope of the SAR and we believe the changes to the standards will provide registered entities with additional options for using other efficient tools for CIP compliance activities.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment.	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
In addition to the mentioned potential modifications for CIP-004-6 R4.1.3, R4.4, R5.3 & CIP-011-2 R1, Tacoma Power recommends the SAR be extended to include review of CIP-004-6 R2.1.5 which covers training for BES Cyber System Information Handling, and CIP-011-2 R2 which deals with preventing unauthorized access to BCSI when a system is being reused or disposed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SAR DT has revised the SAR to more accurately state what the SDT would be addressing with the future proposed revisions.	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
In general, Idaho Power Company agrees with the scope of the SAR as described. BCSI protections should be flexible enough to provide an entity with the ability to adapt to different environments and situations while still being restrictive enough to provide assurance that information is protected in storage, transit, and use.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with the proposed scope of this project, and agrees that additional clarity regarding this issue is sorely needed. **Also, we would be interested to know if the drafting team has considered, or is aware if this project will impact CIP-013 specifically?**	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Support NRECA comments.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see response to NRECA.	
Jeremy Voll - Basin Electric Power Cooperative - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Support NRECA Comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to NRECA.	
Douglas Webb - Westar Energy - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	
Westar and Kansas City Power & Light are supportive of Edison Electric Institute's response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI.	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Exelon agrees with the overall scope of the SAR. There are sections in the document that need clarification. Example #4.X.2, the language "may include but are not limited to…" seems to imply that entities aren't being held to any one thing specifically except identifying "… security protection(s) used to prevent unauthorized access to [BCSI] within each repository". Further define what's expectations are around "Data loss prevention techniques and rights management services" in section 4.X.2. Example #2 4.1.3 "Physical access to physical BES Cyber System Information storage locations;" appears somewhat redundant with 4.1.4, "Physical access to unencrypted electronic BES Cyber System Information storage locations;" where this may require a fairly significant effort.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	

Barry Lawson - National Rural Electric Cooperative Association - 3,4	
Answer	Yes
Document Name	
Comment	
NRECA supports the proposed scope of the SAR and we believe the changes to the standards will provide registered entities with additional options for using other efficient tools for CIP compliance activities.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
OG&E supports the comments made by EEI: Comments: EEI member companies support the intent of the proposed SAR but believe there is room to clarify the draft language to ensure the affected Reliability Standards continue to meet the Reliability needs of the Bulk Electric System. From that perspective, we offer the following brief input for consideration:	

Comments are provided by SAR Section Title:

Industry Need: We recommend removing the introductory statement (i.e., “While there is no direct benefit to the reliability of the BES”), because we believe this statement conflicts with the following text, as currently written.

Purpose or Goal: EEI members offer for consideration the following clarifying edits consideration:

This project is intended to Cclarifying and **expand** the **options available under the** CIP requirements**,** related to BES Cyber System Information access, to **remove unnecessary barriers and** allow for alternative methods, **(e.g.,** such as encryption, etc.), **that could provide equally effective solutions for the storage, transit and access** to be utilized in the protection**ed** of BCSI **data**.

Do you know of any consensus building activities in conjunction with this SAR? EEI member companies ask that conclusions developed by the “informal team” assembled by the NERC Compliance Input Working Group be referenced within this SAR. While it is clear that a large number of SMEs worked on this effort, their findings and recommendations are neither posted by NERC or referenced within this SAR.

Are there alternatives that have been considered or could meet the objectives? EEI member companies question whether the detailed examples contained within the SAR might unintentionally limit the SDT from developing other, possibly more effective, solutions and offer the following edits.

As a means to assist the SDT, several possible options **are provided** for **SDT consideration to address** revision**s** to CIP-004-6 Requirement R4 Part 4.1.3. **These options are not intended to limit the SDT from developing other more effective solutions.**

Additionally, EEI member companies are unclear whether the examples provided were developed as part of the informal team (previously mentioned in the proceeding question), that operated under the direction of the NERC Compliance Input Working Group. If that is the case, we believe such information would be better placed under the proceeding question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI.	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NV Energy supports the project as intended; to expand available options under current Standard related to an entity to utilize changes in technologies for data storage paltforms. That said, we do believe tht further clarifiaction and development still needs to take place to define scope. NV Energy believes the current SAR language is still too general in its statement for allowing Industry and Entities to be more flexible in performing business function and using new technologies, but NV Energy would request more clarifying language to understand the burden of accountability via evidence on the Entity to provide after this change is made. It would benefit NV Energy to know this, prior to agreeing to creation of a SDT for the project. Keeping the subject matter only in the scope of CIP-004 and CIP-011, we agree with a SAR to address a growth for technologies.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SAR DT has made revisions to the scope and we believe your concern has been addressed.	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
While AEP agrees with the proposed scope of the SAR, we recommend that the examples provided for possible revisions to CIP-004-6 Requirement R4 Part 4.1.3 be deleted from the SAR. The inclusion of the examples hinders the flexibility of the SDT to craft the revisons necessary to accurately address the use of encryption on BES Cyber System Information. AEP recommends the SDT work off the scope and objectives as written in the Detailed Description section of the SAR.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company supports the intent of the proposed SAR but believes there is room to clarify the draft language to ensure the affected Reliability Standards continue to meet the Reliability needs of the Bulk Electric System.	

Southern Company requests that the scope of the SAR allows the SDT to specifically address and clarify the interpretation around encrypted BCSI and how encrypted data (cyphertext) does not constitute "information that can be used", as per the BCSI definition. To consider cyphertext to still meet the definition of BCSI is in opposition to the plain language of the existing defined term, and to consider it as such nullifies any benefit to be gained or optionality for using 3rd party hosting solutions as a Registered Entity would have no control over those physically accessing the 3rd party's data centers. Physical access to electronically stored and encrypted cyphertext should be considered outside of the scope of this SAR based on the grounds that access to cyphertext without the ability to decrypt that data should not be considered "access to BCSI." The SAR should also clarify that the inclusion of encryption as an option to secure BCSI is in addition to other acceptable means available to Registered Entities, such as other physical and electronic security controls, and that the SAR will not force the SDT into limiting a Registered Entity's options for complying with the Standard. Southern is concerned that the detailed examples contained within the SAR might unintentionally limit the SDT from developing other, possibly more effective, solutions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions. The SAR DT has revised the scope.	
Jerry Horner - Basin Electric Power Cooperative - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Support NRECA comments.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see response to NRECA.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE suggests adding verbiage to the SAR to indicate entities should use the strongest encryption algorithm since not all encryption algorithms are secure.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Comments: The impact of nondisclosure agreements (NDAs) also should be considered on managing access to BSCI. In some cases within the NERC CIP Standards, a properly constructed NDA apparently can provide sufficient evidence of adequate information handling, and in other cases it cannot. For sensitive CIP-014 documents, for instance, an NDA is explicitly identified within the Standard (R2, R6) as sufficient for protecting the information, and in practice validating the existence of such an NDA appears to be the audit approach for the information protection aspect	

of CIP-014 R2 and R6. There is no effort on the part of ERO auditors to identify CIP-004 R4 and R5 details, such as who has access to the information, when they were disabled, or how or where it is stored by the third party signing the NDA.

Similarly, an NDA appears audit-sufficient for BSCI or sentitive information provided to third party consultants as part of a mock audit, say, or for program improvement work, or for such information shared among regulated entities themselves as necessary for reliable operation of operation of the power grid. To date, NERC CIP auditors do not appear to require or request CIP-004-type evidence of how the third-party handled or stored the sensitive information or BCSI. The existence of the NDA is sufficient.

Finally the ERO enterprise itself provides a third example of how NDAs, by themselves, are sometimes deemed sufficient for third-party handling and storage of sensitive information and BCSI. Here, the general NDA among the entity and regulator is considered sufficient, even for third-party (ERO) storage of sensitive information and BCSI in cloud-based systems such as webCDMS. Again, no CIP-004-type evidence is requested or expected.

In other cases, an NDA is not deemed sufficient. The most obvious case is that an NDA, by itself, does not appear to considered by NERC auditors as sufficient evidence of adequate protection of BCSI provided by an entity to a third-party cloud storage providers. In such cases, whether a proper NDA exists or not, the audit approach typically calls for review of evidence that all CIP-004 R4 and R5 requirements have been met by the third-party cloud provider.

These different audit approaches for sensitive information and BCSI under an NDA raise several questions. Under what conditions is an NDA, alone, sufficient and why? What is the expectation under CIP-004 R4 for BCSI that is protected pursuant to an NDA? Does the NDA authorize blanket access for the company to which it applies, or is individual authorization expected in addition to the NDA? If the former, what is the expectation regarding access tracking, revocations, and reviews? Including NDA issues within the SAR scope may reveal alternative paths towards secure cloud management of BCSI under NERC CIP.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes

Document Name	
Comment	
PSEG supports the proposed scope of the SAR. Proposed changes to the standards would provide industry with more tools and greater flexibility in complying with the CIP standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI member companies support the intent of the proposed SAR but believe there is room to clarify the draft language to ensure the affected Reliability Standards continue to meet the Reliability needs of the Bulk Electric System. From that perspective, we offer the following brief input for consideration: ***Comments are provided by SAR Section Title*:** **Industry Need:** We recommend removing the introductory statement (i.e., "While there is no direct benefit to the reliability of the BES"), because we believe this statement conflicts with the following text, as currently written. **Purpose or Goal**: EEI members offer for consideration the following clarifying edits consideration:	

This project is intended to clarify and **expand the options available under the** CIP requirements**,** related to BES Cyber System Information access, to **remove unnecessary barriers and** allow for alternative methods, **(e.g.,** encryption, etc.) **that could provide equally effective solutions for the storage, transit and access** to protect**ed** BCSI **data**. (*strike throughs removed due to the system not allowing its use*) **Do you know of any consensus building activities in conjunction with this SAR?** EEI member companies ask that conclusions developed by the "informal team" assembled by the NERC Compliance Input Working Group be referenced within this SAR. While it is clear that a large number of SMEs worked on this effort, their findings and recommendations are neither posted by NERC or referenced within this SAR. **Are there alternatives that have been considered or could meet the objectives?** EEI member companies question whether the detailed examples contained within the SAR might unintentionally limit the SDT from developing other, possibly more effective, solutions and offer the following edits. As a means to assist the SDT, several options **are provided** for **SDT consideration to address** revision**s** to CIP-004-6 Requirement R4 Part 4.1.3. **These options are not intended to limit the SDT from developing other more effective solutions.** (*strike throughs removed due to the system not allowing its use*) Additionally, EEI member companies are unclear whether the examples provided were developed as part of the informal team (previously mentioned in the proceeding question), that operated under the direction of the NERC Compliance Input Working Group. If that is the case, we believe such information would be better placed under the proceeding question.
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SAR DT has made revisions to address reliability benefits and made a clarification to provided examples.	
Darcy O'Connell - California ISO - 2 - WECC	
Answer	Yes
Document Name	

Comment	
CAISO proposes that any third party obligations for storing BCSI in the cloud should not be embedded in the requirements but deferred to cloud vendor risk asseements	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT so they can request additional information for clarity.	
Marty Hostler - Northern California Power Agency - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your participation.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Cassie Williams - Golden Spread Electric Cooperative, Inc. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
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	
Thank you for your participation.	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your participation.	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your participation.	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Gregory Campoli - New York Independent System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	
We are in support of the scope of the SAR and believe changes to the standards will give registered entities additional options for using other methods for CIP compliance activities.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

2. Provide any additional comments for the SAR drafting team to consider, if desired.	
Darcy O'Connell - California ISO - 2 - WECC	
Answer	
Document Name	
Comment	

The CAISO offers the following feedback on the SAR.

INDUSTRY NEED SECTION:

CAISO contends that this initiative could have a direct benefit to reliability. The use of third-party solutions (aka cloud) for the storage of BES Cyber System Information can provide a reliability benefit in having recovery plans and other information available to the entity in the event they are needed and the entity's systems are unavailable.

Further, as technologies and cyber attacks advance and become more complex, Responsible Entities are becoming increasingly interested in collecting and correlating electronic access monitoring events across their enterprises. This broad-based information collection provides Responsible Entities with more visibility into emerging threats and trends. Many of these types of software providers are no longer offering on-premises solutions. Allowing the use of third parties for these solutions to analyze and take action serves to improve the overall cybersecurity and reliability of the BES through early detection of compromise.

CAISO would also note that the SAR does not address the use of applications. The SAR only addresses storage. The SAR should account for both.

PURPOSE OR GOAL SECTION:

CAISO contends that encryption is already recognized as a means to protect BCSI. Under CIP-011-2 R2, Part 2.1, encryption is listed as a means to prevent "unauthorized retrieval" of BCSI. Unauthorized retrieval is basically the same concept as unauthorized access. The use of encryption should be applied consistently to CIP-004 R4, CIP-004 R5, and CIP-011 R2, Part 2.1.

DETAILED DESCRIPTION SECTION:

CAISO contends that encryption is already recognized as a means to protect BCSI. Under CIP-011-2 R2, Part 2.1, encryption is listed as a means to prevent "unauthorized retrieval" of BCSI. Unauthorized retrieval is basically the same concept as unauthorized access. The use of encryption should be applied consistently to CIP-004 R4, CIP-004 R5, and CIP-011 R2, Part 2.1. The use of encryption can be used to prevent access. Therefore, CIP-004 R4 and R5 should not apply since access is prevented.

CAISO agrees that audit evidence should be addressed. This should include the use of external audit reports to demonstrate compliance in lieu of detailed evidence that would be available for on-premises implementations. In the context of these services, the Responsible Entity's obligations may only be limited to due diligence in reviewing third party audit and certification details.

ALTERNATIVES SECTION:

CAISO agrees with the concept of Example #1, but requests clarification on the inclusion of "virtual or non-virtual environment" on Example #1.

ADDITIONAL COMMENTS:

One area that should be considered is to address the geographical location of BCSI stored with a third party (aka cloud). Requirements should be drafted for entities to evaluate the geographic location of hosted solutions in their risk assessment of the service.

Any requirement language should include provisions of a CIP Exceptional Circumstance in addressing access controls under CIP-004.

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SAR DT has made revisions to the scope as well as addressing the flexibility and geographical location. This will be noted for the SDT to consider as they draft proposed revisions.	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	

ERCOT offers the following additional comments for the SAR drafting team to consider.

INDUSTRY NEED SECTION

ERCOT believes this initiative could have a direct benefit to reliability. The use of third-party solutions (aka cloud) for the storage of BES Cyber System Information can provide a reliability benefit in having recovery plans and other information available to the entity in the event they are needed and the entity's systems are unavailable.

In addition, as technologies and cyber attacks advance and become more complex, Responsible Entities are becoming increasingly interested in collecting and correlating electronic access monitoring events across their enterprises. This broad-based information collection provides Responsible Entities with more visibility into emerging threats and trends. Many of these types of software providers are no longer offering on-premises solutions. Allowing the use of third parties for these solutions to analyze and take action serves to improve the overall cybersecurity and reliability of the BES through early detection of compromise.

ERCOT also notes that the SAR does not address the use of applications. The SAR only addresses storage. The SAR should take both into consideration.

PURPOSE OR GOAL SECTION

Encryption is already recognized as a means to protect BCSI. Under CIP-011-2 R2, Part 2.1, encryption is listed as a means to prevent "unauthorized retrieval" of BCSI. Unauthorized retrieval is basically the same concept as unauthorized access. The use of encryption should be applied consistently to CIP-004 R4, CIP-004 R5, and CIP-011 R2, Part 2.1.

DETAILED DESCRIPTION SECTION

Encryption is already recognized as a means to protect BCSI. Under CIP-011-2 R2, Part 2.1, encryption is listed as a means to prevent "unauthorized retrieval" of BCSI. Unauthorized retrieval is basically the same concept as unauthorized access. The use of encryption should be applied consistently to CIP-004 R4, CIP-004 R5, and CIP-011 R2, Part 2.1. The use of encryption can be used to prevent access. Therefore, CIP-004 R4 and R5 should not apply because access is prevented.

ERCOT concurs with the SAR drafting team that audit evidence should be addressed. This should include the use of external audit reports to demonstrate compliance in lieu of detailed evidence that would be available for on-premises implementations. In the context of these services, the Responsible Entity’s obligations may only be limited to due diligence in reviewing third party audit and certification details.

ALTERNATIVES SECTION

ERCOT agrees with the concept of Example No. 1, but requests clarification on the inclusion of "virtual or non-virtual environment" in Example No. 1.

ADDITIONAL COMMENTS

An additional area that should be considered is the geographical location of BCSI stored with a third party (aka cloud). Requirements should be drafted for entities to evaluate the geographic location of hosted solutions in their risk assessment of the service. Finally, any new requirement language should include provisions concerning CIP Exceptional Circumstance in addressing access controls under CIP-004.

Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SAR DT has made revisions to the scope as well as addressing the flexibility and geographical location. This will be noted for the SDT to consider as they draft proposed revisions.	
Gregory Campoli - New York Independent System Operator - 2	
Answer	
Document Name	
Comment	

The NYISO offers the following feedback on the SAR.

INDUSTRY NEED SECTION:

NYISO contends that the standard revision should be specific to storage of BCSI. This would include modifications to support the use of encryption as an acceptable level of protection for data being stored within third party infrastructure.

PURPOSE OR GOAL SECTION:

NYISO contends that encryption is already recognized as a means to protect BCSI. Under CIP-011-2 R2, Part 2.1, encryption is listed as a means to prevent “unauthorized retrieval” of BCSI. Unauthorized retrieval is basically the same concept as unauthorized access.

DETAILED DESCRIPTION SECTION:

The use of encryption to ensure both integrity and confidentiality at a minimum should be the focus.

Modifications to the standards should include the establishment of acceptable levels of encryption, the management of keys, the establishment and testing of encryption for data stored and in transit to/from third party providers of cloud storage.

CIP modifications need to provide clarity in establishing what obligations the responsible entity would have in order to establish and maintain compliance and what aspects could be left to the third party provider of cloud storage.

Modifications should include noting contractural provisions that would need to be in place to assure the controls are in place (i.e. testing, alerting) and what obligations the third party provider would have as it pertains to data destruction once contractual relationship is terminated. **ALTERNATIVES SECTION:** NYISO agrees with the concept of Example #1, but requests clarification on the inclusion of "virtual or non-virtual environment" on Example #1. **ADDITIONAL COMMENTS:** One area that should be considered is to address the geographical location of BCSI stored with a third party (aka cloud). Requirements should be drafted for entities to evaluate the geographic location of hosted solutions in their risk assessment of the service. Any requirement language should include provisions of a CIP Exceptional Circumstance in addressing access controls under CIP-004.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SAR DT has made revisions to the scope as well as addressing the flexibility and geographical location. This will be noted for the SDT to consider as they draft proposed revisions.	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	
Document Name	
Comment	

None	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Jerry Horner - Basin Electric Power Cooperative - 1,3,5,6	
Answer	
Document Name	
Comment	
Support NRECA comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to NRECA.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	
If approved, the following is provided as feedback to the NERC SDT that will be addressing the SAR:	

Southern Company suggests the SDT consider modifying the glossary definition of BCSI in the section of the defined term that states what is not BCSI to add language to the effect of “encrypted cyphertext without the ability to decrypt or access the encryption key”. Properly encrypted data is not actual information, but cyphertext and not useable without a “key” to decrypt it.

Southern Company also suggests the SDT consider requirements for the use of two-factor authentication when accessing BCSI stored on 3rd party hosted solutions.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	
Document Name	

Comment
NV Energy shares EEI's comments that conclusions developed by the “informal team” assembled by the NERC Compliance Input Working Group be referenced within this SAR. While it is clear that a large number of SMEs worked on this effort, their findings and recommendations are neither posted by NERC or referenced within this SAR.

Additionally, NV Energy is unclear whether the examples provided were developed as part of the informal team that operated under the direction of the NERC Compliance Input Working Group.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI.	
Barry Lawson - National Rural Electric Cooperative Association - 3,4	
Answer	
Document Name	
Comment	
NRECA appreciates the efforts of Tri-State G&T and the other members of the NERC Compliance Input Working Group for submitting this SAR.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Andy Fuhrman - Minnkota Power Cooperative Inc. - NA - Not Applicable - MRO	
Answer	
Document Name	
Comment	
MPC has additional concerns regarding the ambigious term: "designated storage location". The ultimate objective of CIP-004 R4.1.3 is to protect BCSI, not a server, room, locker, computer, vehicle, etc. BCSI can be anywhere as it is stored, used, and transported. A "designated storage location" is a challenge to define and difficult to audit. A risk-based approach allows an entity to define the risk and the adequacy of	

the actions taken to mitigate that risk, without confining those actions to prescriptive definitions or an out-of-date or restrictive framework. The term "designated storage location" could be removed from CIP-004 altogether, with all requirements for the protection of BCSI being specified within CIP-011 in a manner similar to what is suggested above. *The examples provided in the SAR are restrictive, burdensome, and costly, and do not allow the entity to address the level of risk posed by a particular situation. MPC is strongly opposed to any language that resembles the examples provided in the SAR. The Cost Impact Assessment notes potential savings due to economies of scale. While this my be true when considering the use of cloud storage, the reality is that highly prescriptive requirements such as the examples that are provided, would significantly increase costs without an appropriate risk analysis.*	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SAR DT has addressed the concerns with revisions to the SAR concerning "designated storage location." This will be noted for the SDT to consider as they draft proposed revisions.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	
TVA supports review of the CIP-004 and CIP-011 language as currently written, specifically with regard to the use of encryption in place of physical access controls. However, TVA cautions against including discussion of specific technologies in the language of the standards that could prohibit or discourage innovation or use of emerging technologies.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SAR DT agrees that it should be about the “what” and not the “how”. This will be noted for the SDT to consider as they draft proposed revisions.	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Douglas Webb - Westar Energy - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	

Answer	
Document Name	
Comment	
ACES would like to thank the SAR Team for their efforts and opportunity to comment on the SAR.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jeremy Voll - Basin Electric Power Cooperative - 1,3,5,6	
Answer	
Document Name	
Comment	
Support NRECA Comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to NRECA.	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	
Document Name	
Comment	

Support NRECA comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to NRECA.	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
Agree with the objective of the proposal, but are we certain that the current language of CIP-004-6 Requirement R4 Part 4.1.3 cannot accommodate third-party cloud-based encrypted BCSI? The “or” in “physical or electronic” access to designated storage locations (an undefined term that can be defined by the Responsible Entity) permits electronic authorization exclusively, relieving the Responsible Entity of any physical access concerns. Encryption key management can be the process to authorize electronic access to BCSI. The designated storage location could be defined as the Responsible Entity’s encrypted BSCI in a designated third-party data repository. Does the requirement language need to be changed to explicitly permit, or can other options be pursued to ascertain whether or not current language can accommodate? Has anyone submitted implementation guidance for ERO endorsement showing how industry believes this can be done compliantly? If NERC is receptive to encryption satisfying R4.1.3, a SAR may yet be required to specify minimum acceptable encryption key strength, such as NIST Advanced Encryption Standard AES 256-bit, just as minimum password length and complexity requirements are set forth in CIP-007-6 R5.5	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SAR DT asserts that revisions to the current standards are needed to provide further clarity.	
Oliver Burke - Entergy - Entergy Services, Inc. - 1	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy would like to recommend that the drafting team consider the potential impacts of setting encryption at the document level or the repository level.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	
Comment	

Reclamation recommends IT systems that store BCSI be certified and accredited for operation in accordance with federal and Department of Homeland Security (DHS) standards. Boundaries and security authorization(s) must be defined for systems with common security controls. National Institute of Standards and Technology (NIST) Information Management Security suggests entities should control risks by evaluating the system's or information's importance and designating the confidentiality, integrity, and availability necessary for the system or information. The entity's CIP Senior Manager or delegate should accept (approve) the risk for the responsible entity.

Additionally, the revised standards must specifically account for the requirements pertaining to Controlled Unclassified Information (CUI) in 32 CFR 2002. Reclamation recommends the SDT obtain a full understanding of overall information protection requirements, to include requirements beyond IT systems. For example, there is no mechanism to encrypt hard copy data, so physical protection requirements cannot be totally removed.

Reclamation also recommends the SDT incorporate the following definition of "Information Security" as stated in NIST SP800-12r1, *Section 1.4 Important Terminology,* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf:

"Information Security – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability."

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	

Document Name	
Comment	
GSOC appreciates the efforts of Tri-State G&T and the other members of the NERC Compliance Input Working Group for submitting this SAR. Drafting team should consider how entities and NERC could rely on third party audit assessment of cloud services provider. They should also evaluate the requirement for access management, revocation, disposal and information protection.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
SRP agrees with the SAR that additional considerations need to be given to other ways to protect BCSI beyond access to storage locations. There are more methods to protect BCSI and the standards need to be flexible enough to allow it. The current requirements apply to BCSI in the cloud, however, it is not feasible to expect third party providers of hosted solutions (cloud BCSI storage locations) to comply with CIP-004-06 R4.1.3 and CIP-004-6 R5.3, so entities have to look for other options – and not using cloud providers is no longer an option. SRP suggests the SDT look for opportunities to update CIP-011 requirements to better document the types of protections in place for BCSI storage locations where the only available control is CIP-004-6 (access management), then CIP-004 applies. SRP disagrees with an approach that encryption or masking BCSI renders it no longer BCSI. This would create a need for entities to know when information is no longer BCSI (upon encryption) and when it becomes BCSI again (upon decryption). It will be difficult to apply the	

current CIP-004 storage locations based requirements. SRP agrees with the SAR's approach that the standards should be updated to allow for other methods to protect BCSI. This will ensure a complete inventory of BCSI and a better overall understanding of the protections in place. The SDT may want to consider minimum requirements (or guidance) for an approach to properly sanitize (i.e. cryptographic erase) off premise BCSI.	
Likes 1	Minnkota Power Cooperative Inc., NA - Not Applicable, Fuhrman Andy
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro	
Answer	
Document Name	
Comment	

Given that the Example #2 proposes a reasonable and alternative approach that permits encryption and key management to be utilized in lieu of physical/electronic access controls, we support Example #2 to be considered for modifying CIP-004-6 R4 Part 4.1.3. This encryption and key management method woud provide flexibility for entities to manage BCSI access and facilitate the cloud storage solution. Note that if the CIP-004-6 R4 Part 4.1.3 is revised using Example #2, the CIP-004-6 R4 Part 4.3 and R5 Part 5.3 should be revised in accordance with the modification of CIP-004-6 R4 Part 5.1.3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	
Document Name	
Comment	
The standards development team should favor non-prescriptive standards for protection of BES Cyber System Information that requires an appropriate level security within (1) individual Entities, (2) Application Providers, (3) Public Cloud Providers, (4) Entities that hold protected information for other utilities business partners, and (5) business partners that need access and temporarily retain this information.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SAR DT has made revisions to the scope as well as addressing the flexibility. The SDT should consider issues related to where data resides (e.g. off premises). This will be noted for the SDT to consider as they draft proposed revisions.	