NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2023-04 Modifications to CIP-003 | Draft 1
Comment Period Start Date:	10/24/2023
Comment Period End Date:	12/7/2023
Associated Ballot(s):	2023-04 Modifications to CIP-003 CIP-003-A IN 1 ST 2023-04 Modifications to CIP-003 Implementation Plan IN 1 OT

There were 63 sets of responses, including comments from approximately 165 different people from approximately 104 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, 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, contact Director, Standards Development Latrice Harkness (via email) or at (404) 858-8088.

Questions

1. Do you agree with the language proposed in CIP-003-A Attachment 1? If you do not agree, please provide recommended language you would support and, if appropriate, technical or procedural justification.

2. Do you agree with the language proposed in CIP-003-A Attachment 2? If you do not agree, please provide recommended language you would support and, if appropriate, technical or procedural justification.

3. The Standard Drafting Team (SDT) proposes a three (3) year implementation plan for CIP-003-A. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with detailed explanation.

4. The SDT believes the language of CIP-003-A addresses the issues outlined in the SAR in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

5. Provide any additional comments on the standard and technical rationale for the SDT 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
MRO	Anna Martinson	1,2,3,4,5,6	MRO	MRO Group	Shonda McCain	Omaha Public Power District (OPPD)	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Jay Sethi	Manitoba Hydro (MH)	1,3,5,6	MRO
					Jaimin Patal	Saskatchewan Power Corporation (SPC)	1	MRO
					Kimberly Bentley	Western Area Power Adminstration	1,6	MRO
					Marc Gomez	Southwestern Power Administration (SWPA)	1	MRO
					Fred Meyer	Algonquin Power Co.	3	MRO

					George Brown	Pattern Operators LP	5	MRO
					Larry Heckert	Alliant Energy (ALTE)	4	MRO
					Terry Harbour	MidAmerican Energy Company (MEC)	1,3	MRO
					Bryan Sherrow	Board Of Public Utilities (BPU)	1	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Michael Ayotte	ITC Holdings	1	MRO
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	TVA RBB	Ian Grant	Tennessee Valley Authority	3	SERC
					David Plumb	Tennessee Valley Authority	1	SERC
					Armando Rodriguez	Tennessee Valley Authority	6	SERC

					Nehtisha Rollis	Tennessee Valley Authority	5	SERC
Chris Carnesi	Chris Carnesi		WECC	NCPA	Marty Hostler	Northern California Power Agency	4	WECC
					Dennis Sismaet	Northern California Power Agency	6	WECC
WEC Energy Group, Inc.	Christine Kane	3		WEC Energy Group	Christine Kane	WEC Energy Group	3	RF
					Matthew Beilfuss	WEC Energy Group, Inc.	4	RF
					Clarice Zellmer	WEC Energy Group, Inc.	5	RF
					David Boeshaar	WEC Energy Group, Inc.	6	RF
Manitoba Hydro	Jay Sethi	1,3,5,6	MRO	Manitoba Hydro Group	Nazra Gladu	Manitoba Hydro	1	MRO
					Mike Smith	Manitoba Hydro	3	MRO
					Kristy-Lee Young	Manitoba Hydro	5	MRO
					Kelly Bertholet	Manitoba Hydro	6	MRO
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC

					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					John Nierenberg	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,RF,SERC,Texas RE,WECC	ACES Collaborators	Bob Soloman	Hoosier Energy Electric Cooperative	1	RF
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Nikki Carson-Marquis	Minnkota Power Cooperative, Inc.	1	MRO

					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
Eversource Energy	Joshua London	1		Eversource	Joshua London	Eversource Energy	1	NPCC
					Vicki O'Leary	Eversource Energy	3	NPCC
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
					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Alain Mukama	Hydro One Networks, Inc.	1	NPCC

Deidre Altobell	Con Edison	1	NPCC
Jeffrey Streifling	NB Power Corporation	1	NPCC
Michele Tondalo	United Illuminating Co.	1	NPCC
Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC
Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
Randy Buswell	Vermont Electric Power Company	1	NPCC
James Grant	NYISO	2	NPCC
John Pearson	ISO New England, Inc.	2	NPCC
Harishkumar Subramani Vijay Kumar	Independent Electricity System Operator	2	NPCC
Randy MacDonald	New Brunswick Power Corporation	2	NPCC
Dermot Smyth	Con Ed - Consolidated	1	NPCC

	Edison Co. of New York		
David Burke	Orange and Rockland	3	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
David Kwan	Ontario Power Generation	4	NPCC
Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
Glen Smith	Entergy Services	4	NPCC
Sean Cavote	PSEG	4	NPCC
Jason Chandler	Con Edison	5	NPCC
Tracy MacNicoll	Utility Services	5	NPCC

					Shivaz Chopra	New York Power Authority	6	NPCC
					Vijay Puran	New York State Department of Public Service	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					David Kiguel	Independent	7	NPCC
					Joel Charlebois	AESI	7	NPCC
					Joshua London	Eversource Energy	1	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion	5	NA - Not Applicable

						Resources, Inc.		
Steve Toosevich	Steve Toosevich			NIPSCO Compliance	Steven Taddeucci	NiSource - Northern Indiana Public Service Co.	3	RF
					Kathryn Tackett	NiSource - Northern Indiana Public Service Co.	5	RF
					Joseph OBrien	NiSource - Northern Indiana Public Service Co.	6	RF
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC
					Charles Norton	Sacramento Municipal Utility District	6	WECC

					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC
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

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

					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. Do you agree with the language proposed in CIP-003-A Attachment 1? If you do not agree, please provide recommended language you would support and, if appropriate, technical or procedural justification.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	
Section 3.1, specifically 3.1.3, is limited to the means of authentication that can be used. The standard needs to allow for a LIBCS Intermediate System equivalent. If a person could authenticate to the LIBCS Intermediate System, then remote access could be permitted from it to the Cyber Assets at the Low Impact Asset. Not all field devices support authentication, and this would help provide a means of authentication before connecting. PNMR also supports EEI's comments pertaining to Section 3, parts 3.1.4 and 3.1.6.	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can "utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s)." The SDT changed 3.1.3 so that authentication can occur for a "network(s)" meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the "asset containing" or the authentication source used in 3.1.3 (such as an Intermediate System). See EEI response.	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	

Regarding the definition of 3.1's scope, the specification of "connectivity that provides the ability to communicate" is confusing and has no opposite state; connectivity in this context implies communication. The addition of "of Protection systems" to iii is also unnecessarily expansive. Language recommendation:

3.1 For routable connectivity:

I. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving a defined perimeter containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., IEC 61850, etc.)

Regarding section 3.1.2, that subsection implies deployment of Intrusion Protection Systems (IPS) at every low impact BES Cyber System for any "connection to communicate". This is technically infeasible for many communication types (e.g., RS-232, RS-485, non-IP IEC 61850, etc.). It would necessitate building routable connectivity to many systems that otherwise do not require it, do not have it, and may be difficult or expensive to build out (see cost feasibility below) simply to deploy a monitoring solution. The added communication risk combined with cost is not an effective risk-based approach to securing low impact BES.

Regarding section 3.1.4, this requirement is overly prescriptive and makes certain assumptions about how connections for communications may be authorized, secured, and used. The requirement should address a security concern topically – e.g. "ensure communications are protected appropriately given a risk-based approach".

Regarding sections 3.1.5 and 3.1.6, we agree with the EEI comments and further assert that the undefined use of "remote access" is problematic and should be scoped to certain types of routable communications Overall, concerns with communication monitoring for low impact BES should be addressed in a risk-based and architecture-based approach rather than a BES location approach specifically because of their lower impact. For example, rather than mandating IPS monitoring and user disablement at a low impact BES, require that interactive remote access be controlled and monitored from central aggregation or choke points (or an architecturally equivalent

concept) and allow the entities to determine a risk-based security partitioning and control plan based on factors within their own environment.

In addition, **FirstEnergy supports EEI's comments** which state:

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR; these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authentical and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect BES Cyber System network authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.16 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	
Response	
Change made to structure. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification." See EEI response.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute for question #1.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	

Answer	No
Document Name	
Comment	
AECI is supportive of the approach to consolidate to the electronic access section as adding a new section to capture these revisions would be purely duplicative. I also think that the new revisions are drafted in a way that allows for utilizing solutions that may be put in place for the version 9 for these new revisions if desired but also allowing for separate solutions if needed. The only concern with the current draft language is the use of the following phrase: "to mitigate risks associated with electronic access" in the intro paragraph of Section 3. As written there is a signifigant potential to cause more scrutiny on the allowed communications that did not previously exist and was not part of the SAR, and would give total discression to auditor interpretation.	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification."	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The number of Low Impact BES Cyber Systems impacted would make achieving compliance burdensome in terms of level of effort, cost, and required technology implementations.	

Likes 0	
Dislikes 0	

Response

The revisions to CIP-003-9 were made based on the scope of the approved SAR, and the SDT appreciates that there may be cost associated with the implementation of the new standard. The SDT has kept the requirements to a level of granularity that is either the "asset containing low impact BCS" or "networks containing low impact BCS" so that it does not go down to the level of individual BCS or device. The intent is the monitoring of traffic and authentication of users at a higher level than each system due to the large scope of lows.

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

Answer	No
Document Name	

Comment

To accommodate those systems that do not have the capability to perform the required function, such as protecting user authentication information in transit, Tacoma Power recommends including language in Attachment 1, Section 3, such as "per system capability," as found throughout the rest of the CIP Standards. Specifically, Tacoma Power recommends adding the "per system capability" to the lead in to Section 3 of Attachment 1.

Suggested lead in language update:

"Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, to mitigate risks associated with electronic access, the Responsible Entity shall implement controls, **per system capability**, to:"

Additionally, Tacoma Power has a concern that Attachment 1, Section 3 Part 3.1.3 can be read in multiple ways. Specifically as it relates to the (i.) and (ii.) language in the lead-in to Section 3.1 (excerpt as follows):
3.1 For connectivity that provides the ability to communicate:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

What does the phrase "**each instance** of electronic remote access to **networks** containing low impact BES Cyber Systems" mean in Part 3.1.3? We see that the TR includes the desire to allow initial authentication to the network to allow transition to sub-networks, etc. But there is no structure for this within the 3.1 (i.) and (ii.) construct. Tacoma Power is concerned that the language of 3.1.3 does not support the idea of allowed sub-network connections without additional authentication if they are to a different asset containing a low impact BCS, since this ties it back to the original (i.)

In the scenario where a relay tech logs into a central system which includes configurations to access relays at several substations, is that relay tech required to re-authenticate each time they access a relay at a different substation (i.e., at a different asset containing Low Impact BCS)? The language of the Requirement does not provide clarity to this situation.

To aid in this scenario, Tacoma Power suggests the following language for clarity of Attachment 1 Section 3 Part 3.1.3:

"3.1.3 Authenticate users when remotely accessing networks containing low impact BES Cyber Systems."

Likes 1	LaKenya Vannorman, N/A, Vannorman LaKenya
Dislikes 0	

Response

1. The SDT has not included "per system capability" within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the "networks containing" or "asset containing level". The SDT also clarified the Section 3 language to also incorporate "Intermediate System" style implementations as well.
2. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can "utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s)." The SDT changed 3.1.3 so that authentication can occur for a "network(s)" meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the "asset containing" or the authentication source used in 3.1.3 (such as an Intermediate System).

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments. Dominion Energy supports in part the proposed changes to CIP-003-A Attachment 1, but disagree with the addition of proposed 3.1.5 and 3.1.6 and the deletion of Section 6. First, the SAR only authorized the change to Section 3 and the current language in Section 6 is clearer than what is proposed. We suggest deleting 3.1.5 and 3.1.6 and restoring Section 6 to address the concerns.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Change made. The SDT has reviewed your comment and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access.	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	No
Document Name	
Comment	
Eversource agrees with the comments of EEI.	

Likes 0	
Dislikes 0	
Response	
See EEI response.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
The NERC Low Impact Criteria Review Report mentions the risk of coordinated attacks on low impact BES Cyber Systems that could adversely affect the BES. However, coordinated attacks are not considered for categorization of BES Cyber Systems in CIP-002, and the proposed language in CIP-003 is placing more restrictive controls on low impact BCS than medium impact BCS without ERC. For example, in 3.1.4, protecting user authentication information all the way to the asset is more restrictive than the current requirements for high and medium impact BCS, where an Intermediate System authenticates the user who is then allowed to then access high/medium impact BCS as needed. While the risk to a coordinated attack to multiple low impact BCS is not zero, the restrictive and prescriptive controls proposed does not allow a Responsible Entity to determine the best way to protect its low impact BCS. In 3.1.3, the language “each instance” is ambiguous and should be removed to avoid confusion or misinterpretation. Also, the lack of a clear definition of remote access further adds to the ambiguity and should be clarified or defined. “Per Cyber System/Asset capability” should be added to address those cyber assets that have limitations or cannot be replaced/upgraded without significant expense.	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would	

not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the "asset containing" or the authentication source used in 3.1.3 (such as an Intermediate System).

The SDT has not included "per system capability" within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the "networks containing" or "asset containing level". The SDT also clarified the Section 3 language to also incorporate "Intermediate System" style implementations as well.

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	No
Document Name	
Comment	

Manitoba Hydro recognizes the standard drafting team's effort to develop a draft that clearly outlines requirements meeting the objectives of the project. There appears to be a disconnect in the two requirements to authenticate access and protect this information in transit.

Requirement 3.1.3 requires that access be authenticated at the time of permitting that access to the network containing low impact BES Cyber Systems. This requirement is worded flexibly to allow a number of technical solutions to accomplish the security objective. Requirement 3.1.4 specifies that authentication information be protected in transit from the asset containing low impact BES Cyber Systems. The implementation of 3.1.3 may be configured to have a central point of authentication that is not located at the asset. The text of 3.1.4 takes away flexibility in implementation. The following text is suggested based on the currently accepted wording in CIP-005 for Medium Impact Cyber Assets:

For all instances of electronic remote access to networks containing low impact BES Cyber Systems, protect user authentication information in transit in between the remote client and the authentication system used to meet 3.1.3.

The intent of requirement 3.1.6 is clear, however as currently worded it seems to require all vendor remote access to be disabled at all times. Manitoba Hydro suggests the following wording:

Have a documented method to disable vendor electronic remote access, where vendor electronic remote access is permitted.	
Likes 0	
Dislikes 0	

Response

Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can "utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s)." The SDT changed 3.1.3 so that authentication can occur for a "network(s)" meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the "asset containing" or the authentication source used in 3.1.3 (such as an Intermediate System).

Thank you for your comment. Change made. The SDT has reviewed your comments and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access.

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	

Comment

With new language there will be a large amount of Low Impact BES Cyber Systems impacted. It would be costly for utilities to meet compliance and more burdensome than medium and high impact requirements.

Likes 0	
Dislikes 0	

Response
No change. The SDT notes that the required cyber security program for lows is not stricter than the required program for mediums w/o ERC. Medium impact BCS are subject to all relevant cyber security requirements in CIP-003 through CIP-013, whereas low impact systems are only subject to the requirements in CIP-003, which are not down to individual cyber systems' level. Medium impact BCS w/o ERC have a reduced remote access attack surface, yet still have more requirements on the individual cyber systems throughout the CIP standards. The SDT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums.

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
Section 3 in att 1 does not make grammatical sense nor does it flow. There is concern for auditor interpretation to vary. In addtion, SRP is in support of Tacoma Power's comment on the suggested language as it can be interpreted in multiple ways.	
Likes 0	
Dislikes 0	

Response
Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.

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

1. Section 3.1.2 creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers: the proposed language requires detection of known/suspected malicious communications for "inbound and outbound electronic remote access." There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5).

BPA suggests that this requirement be removed for better consistency with the requirements for Medium BCS.

2. Section 3.1.4 creates a higher compliance bar for Low BCS than for Medium BCS: in the latest Draft 5 of CIP-005-8 R2.2 - 2.3, the proposed requirements include only Interactive Remote Access, or human-initiated access. Section 3.1.4 includes all "information in transit to or from the asset containing low impact BES Cyber Systems."

BPA suggests that this requirement be aligned with the latest Draft 5 of CIP-005-8 R2.2 - 2.3: "3.1.4 Protect user authentication *of IRA communications* in transit to or from the asset containing low impact BES Cyber Systems."

3. Section 3.1.6: While BPA appreciates the committee's intent to "present a single section for all electronic access" (Technical Rationale, p. 2), Section 3.1.6 is nonetheless awkwardly worded. It either suggests that all vendor remote access should be disabled (rather than requiring controls that could provide an option to disable vendor remote access), or it contradicts itself in a nonsensical sentence by saying that when vendor access is permitted, it should always be disabled.

BPA suggests aligning with the language used in Draft 5 of CIP-003-10, such as "Have one or more methods" for determining and disabling vendor remote access sessions.

Likes 0	
Dislikes 0	

Response

1. No change. The revisions made to 3.1.2 are within the scope of the SAR.

2. Change made. Added “user-initiated instances” to the language. The DT chose not to specifically use the IRA, because of the relation with Medium/Highs and verbiage in the definition. Additionally, an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).”
3. The SDT has reviewed your comments and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access.”

   Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	No
Document Name	
Comment	
Please clarify whether vendor electronic remote access includes cases involving protocol transition between serial and TCP/IP.	
Likes 0	
Dislikes 0	
Response	
No change. This is specified in Section 3.1 (ii). The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and	

modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR; these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authentical and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect **user BES Cyber System network** authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.16 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	

Response

See EEI response.

Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt

Answer	No
Document Name	

Comment

Black Hills Corporation agrees with the comments below from EEI, FE, and PNM Resources – Public Service Company of New Mexico.

Section 3.1, specifically 3.1.3, is limited to the means of authentication that can be used. The standard needs to allow for a LIBCS Intermediate System equivalent. If a person could authenticate to the LIBCS Intermediate System, then remote access could be permitted from it to the Cyber Assets at the Low Impact Asset. Not all field devices support authentication, and this would help provide a means of authentication before connecting.

Regarding sections 3.1.5 and 3.1.6, we agree with the EEI comments and further assert that the undefined use of “remote access” is problematic and should be scoped to certain types of routable communications. Overall, concerns with communication monitoring for low impact BES should be addressed in a risk-based and architecture-based approach rather than a BES location approach specifically because of their lower impact. For example, rather than mandating IPS monitoring and user disablement at a low impact BES, require that interactive remote access be controlled and monitored from central aggregation or choke points (or an architecturally equivalent

concept) and allow the entities to determine a risk-based security partitioning and control plan based on factors within their own environment.

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR; these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authenticate and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect **BES Cyber System network** authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.1.6 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	
Response	
See EEI, FE and PNM Resources responses.	
Micah Runner - Black Hills Corporation - 1	
Answer	No
Document Name	
Comment	

Black Hills Corporation agrees with the comments below from EEI, FE, and PNM Resources – Public Service Company of New Mexico.

Section 3.1, specifically 3.1.3, is limited to the means of authentication that can be used. The standard needs to allow for a LIBCS Intermediate System equivalent. If a person could authenticate to the LIBCS Intermediate System, then remote access could be permitted from it to the Cyber Assets at the Low Impact Asset. Not all field devices support authentication, and this would help provide a means of authentication before connecting.

Regarding sections 3.1.5 and 3.1.6, we agree with the EEI comments and further assert that the undefined use of "remote access" is problematic and should be scoped to certain types of routable communications Overall, concerns with communication monitoring for low impact BES should be addressed in a risk-based and architecture-based approach rather than a BES location approach specifically because of their lower impact. For example, rather than mandating IPS monitoring and user disablement at a low impact BES, require that interactive remote access be controlled and monitored from central aggregation or choke points (or an architecturally equivalent concept) and allow the entities to determine a risk-based security partitioning and control plan based on factors within their own environment.

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR;

these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authenticate and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect **BES Cyber System network** authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.1.6 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	

Response
See EEI, FE and PNM Resources responses.

Carly Miller - Carly Miller On Behalf of: Sheila Suurmeier, Black Hills Corporation, 5, 6, 1, 3; - Carly Miller	
Answer	No

Document Name	
Comment	

Black Hills Corporation agrees with the comments below from EEI, FE, and PNM Resources – Public Service Company of New Mexico.

Section 3.1, specifically 3.1.3, is limited to the means of authentication that can be used. The standard needs to allow for a LIBCS Intermediate System equivalent. If a person could authenticate to the LIBCS Intermediate System, then remote access could be permitted from it to the Cyber Assets at the Low Impact Asset. Not all field devices support authentication, and this would help provide a means of authentication before connecting.

Regarding sections 3.1.5 and 3.1.6, we agree with the EEI comments and further assert that the undefined use of "remote access" is problematic and should be scoped to certain types of routable communications. Overall, concerns with communication monitoring for low impact BES should be addressed in a risk-based and architecture-based approach rather than a BES location approach specifically because of their lower impact. For example, rather than mandating IPS monitoring and user disablement at a low impact BES, require that interactive remote access be controlled and monitored from central aggregation or choke points (or an architecturally equivalent concept) and allow the entities to determine a risk-based security partitioning and control plan based on factors within their own environment.

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR; these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authenticate and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would

only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect **BES Cyber System network** authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.1.6 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	

Response

See EEI, FE and PNM Resources responses.

Josh Combs - Black Hills Corporation - 3

Answer	No
Document Name	

Comment

Black Hills Corporation agrees with the comments below from EEI, FE, and PNM Resources – Public Service Company of New Mexico.

Section 3.1, specifically 3.1.3, is limited to the means of authentication that can be used. The standard needs to allow for a LIBCS Intermediate System equivalent. If a person could authenticate to the LIBCS Intermediate System, then remote access could be

permitted from it to the Cyber Assets at the Low Impact Asset. Not all field devices support authentication, and this would help provide a means of authentication before connecting.

Regarding sections 3.1.5 and 3.1.6, we agree with the EEI comments and further assert that the undefined use of "remote access" is problematic and should be scoped to certain types of routable communications. Overall, concerns with communication monitoring for low impact BES should be addressed in a risk-based and architecture-based approach rather than a BES location approach specifically because of their lower impact. For example, rather than mandating IPS monitoring and user disablement at a low impact BES, require that interactive remote access be controlled and monitored from central aggregation or choke points (or an architecturally equivalent concept) and allow the entities to determine a risk-based security partitioning and control plan based on factors within their own environment.

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR; these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authenticate and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect **BES Cyber System network** authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.1.6 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	

Response

See EEI, FE and PNM Resources responses.

Ben Hammer - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

Remove Requirement 2 from the standard all together, add in requirements of attachment 1 for low impact BES Cyber systems into the correct CIP standard, CIP-004, CIP-006, CIP-005, CIP-008, and CIP-010 as needed.

There is no definition for the word communicate. This needs to be defined or changed to use the correct terminology.

The language “using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and” is not clear as written. As an example, an entity can have a routable protocol that enters the low impact asset, that never communicates using a bidirectional routable protocol with any Low impact BES Cyber Assets. This creates an undue burden for Registered entities to protect assets that have no routable connectivity.

The definition of vendor needs to be defined and **should not** include long-term /fulltime contract employees that work for the Registered entity.	
Likes 0	
Dislikes 0	
Response	
1. The SDT is not authorized in the SAR to revise all of the standards listed. By having the low impact contained in CIP-002 and CIP-003, this allows "low impact only Entities" to comply with those two standards. 2. The items under 3.1 (i) (ii) and (iii) are to be read as an AND statement. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification. 3. The SDT does not intend to define the term vendor. Please see Project 2020-03 Technical Rationale.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
As proposed, CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4 does not consider per Cyber System capability and may create an impossibility to comply within the implementation timeline without wholesale upgrades or replacements of technology and communications infrastructure. While this newly proposed Requirement Part is consistent with the LICRT report and the subsequent approved SAR; protections from the user all the way through to the asset containing the BCS imposes a mandatory obligation for low impact that is above and beyond the current enforceable requirements set forth for high and medium impact BCS, and also precludes the use of established and current	

enforceable concepts used to protect user authentication information for high and medium impact like IRA through an Intermediate System.

The protections for user authentication information in transit between a user and a high or medium impact BCS are between the user and the Intermediate System, and do not extend all the way to the asset containing the high or medium impact BCS. Here, user authentication information is protected between the initiating device and the Intermediate System, and once authenticated to the Intermediate System, the Requirement language would permit the use of any protocol the entity chooses (Telnet, for example) to make the connection from the Intermediate System to the BCS. Proxied connections/new sessions established from the Intermediate System to the BCS are permitted to transverse unencrypted communication links and use unencrypted protocols (which may be the only method depending on the entity's technology). If "Telnet" is the only method that can be used, there is also no obligation to block clear test interactive protocols from going through a high or medium impact ESP if they are needed, nor to force a VPN tunnel or communication link encryption to do so.

There is no obligation to "protect user authentication information" all the way to the asset containing the BCS for high and medium impact, and to mandate this for low impact does not seem commensurate with risk. CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as written, would only permit the use of an Intermediate System if the Intermediate System were physically located within the asset containing the LBCS, instead of permitting entities to leverage existing centralized infrastructure already implemented for the purpose of protecting user authentication information for high or medium impact.

NSRF requests further SDT consideration of the addition of "per Cyber System capability" language, and the addition of options that would permit protection of user authentication information in transit between the user and an Intermediate System, or the asset containing low impact BES Cyber Systems.

The SAR only directed "protection of user authentication information in transit for **remote access to networks** containing low impact BES Cyber Systems." This would only include network access credentials which could be authenticated locally, precluding the need for these credentials to transit to the asset containing low impact BCS's. Thus, current implementations could remain compliant according to the direction of the SAR.

The proposed language of 3.1.4 expands the SAR mandate to protect all authentication information, which includes account passwords of the low impact BCS's, which requires transmitting these credentials to the BCS's. It is the expansion of the scope of the SAR regarding which credentials need to be protected that makes the proposed 3.1.4 language incompatible with current compliant practices.

If 3.1.4 were re-worded from *"Protect user authentication information"* to *"Protect network authentication information,"* this would expand compliance options to include local authentication and avoid having to send network credentials to the asset.

NSRF offers the following potential language for SDT consideration:

3.1.4 Protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems if using public communication links;

3.1.4 Protect user authentication information in transit to the asset containing low impact BES Cyber Systems, unless low impact BES Cyber System remote access is already protected by going through an Intermediate System meeting the collective requirement parts of CIP-005-7 Requirement R2; if using public communication links, protect user authentication information in transit to and from the asset containing low impact BES Cyber Systems;

3.1.4 Protect user authentication information in transit:

- *BES Cyber Systems if to or from the asset containing low impact using public communication links; or*
- *to the asset containing the low impact BES Cyber Systems if using private communication links, unless low impact BES Cyber System remote access is already protected by going through an Intermediate System meeting the collective requirement parts of CIP-005-7 Requirement R2.*

3.1.4 For all instances of electronic remote access to networks containing low impact BES Cyber Systems, protect user authentication information in transit in between the remote client and the authentication system used to meet 3.1.3.

Likes 1	Corn Belt Power Cooperative, 1, brusseau Larry
Dislikes 0	

Response

1. The SDT has not included "per system capability" within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the "networks containing" or "asset containing level". The SDT also clarified the Section 3 language to also incorporate "Intermediate System" style implementations as well.
2. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can "utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact

cyber security plan(s)." The SDT changed 3.1.3 so that authentication can occur for a "network(s)" meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the "asset containing" or the authentication source used in 3.1.3 (such as an Intermediate System).	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is in support of EEIs response to this question.	
Likes 0	
Dislikes 0	

Response	
See EEI response.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	

LCRA seeks clarification on what “outbound electronic remote access” means. Additionally, the use of the word “remote” throughout the entirety of Section 3 seems inappropriate when discussing the various types of electronic access communications.

We are confused with the roman numerals in section 3.1 that are used to define applicability. LCRA believes that the electronic access being defines here would better be served by a NERC Glossary of Terms definition. This would enable this section to read more clearly.

Section 3.1.2 requires stronger controls than medium impact BES Cyber Systems not at Control Centers. This goes against the Brightline criteria.

Section 3.1.3 requires that authentication occurs when permitting each instance of electronic remote access. LCRA is concerned with the scoping of this requirement when managing connection over Wide Area Network (WAN). It is unclear if intermediate systems or equivalent could be used to achieve compliance.

Section 3.1.5 & 3.1.6 consider restructuring the sentences to avoid confusion. LCRA suggests the following revision:

* 3.1.5 – Implement measures to determine vendor electronic remote access

* 3.1.6 – Implement measures to disable vendor electronic remote access, where enabled

Likes 0	
Dislikes 0	
Response	

1. Change made. The SDT removed the term “remote” from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1.
2. Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.
3. The SDT notes that the required cyber security program for lows is not stricter than the required program for mediums w/o ERC. Medium impact BCS are subject to all relevant cyber security requirements in CIP-003 through CIP-013, whereas low impact systems are only subject to the requirements in CIP-003, which are not down to individual cyber systems’ level. Medium impact BCS w/o ERC have a reduced remote access attack surface, yet still have more requirements on the individual cyber systems throughout the CIP standards. The SDT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums.
4. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System).
5. Change made. The SDT has reviewed your comments and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access.

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	

LCRA seeks clarification on what “outbound electronic remote access” means. Additionally, the use of the word “remote” throughout the entirety of Section 3 seems inappropriate when discussing the various types of electronic access communications.

We are confused with the roman numerals in section 3.1 that are used to define applicability. LCRA believes that the electronic access being defines here would better be served by a NERC Glossary of Terms definition. This would enable this section to read more clearly.

Section 3.1.2 requires stronger controls than medium impact BES Cyber Systems not at Control Centers. This goes against the Brightline criteria.

Section 3.1.3 requires that authentication occurs when permitting each instance of electronic remote access. LCRA is concerned with the scoping of this requirement when managing connection over Wide Area Network (WAN). It is unclear if intermediate systems or equivalent could be used to achieve compliance.

Section 3.1.5 & 3.1.6 consider restructuring the sentences to avoid confusion. LCRA suggests the following review:

- 3.1.5 – Implement measures to determine vendor electronic remote access
- 3.1.6 – Implement measures to disable vendor electronic remote access, where enabled

Likes 0	
Dislikes 0	

Response

See LCRA response above.

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

Answer	No
Document Name	

Comment

AEPC has signed on to ACES comments below:

ACES feels, “Section 3.1.4 Protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems”, should read: Protect electronic remote access information in transit to or from the asset containing low impact BES Cyber Systems;” The addition of authentication of remote users we are fine with, but the SDT chose to just scope in protection of remote user authentication information and we feel that is not the only thing that should be protected. Just like in the case of detection of vendor communication versus all communications (fixed in this version), we feel ALL electronic remote access information should be protected just as it is in CIP-005 R2 if it’s FERC/NERC’s intention of reducing overall cybersecurity risk with this change. Without fully protecting the entire remote access session, risks are only minimally reduced and this standard will have to be revised again to meet the objective.	
Likes 0	
Dislikes 0	
Response	
See ACES response.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
SMUD and BANC appreciate the Standards Drafting Team’s efforts to revise Attachment 1. Section 3.1.1 reads “Permit only necessary inbound and outbound remote electronic access as determined by the responsible entity.” Using the word “remote” in this section narrows the scope of Electronic Access Controls to only inbound and outbound electronic access that is “remote access.” The technical rationale is incorrect in that using this wording does not “maintain the original language used in CIP-003-9, Section 3.1” as CIP-003-9 is more specific.	

We feel there is no need to use the word “remote” in Section 3.1.1 as it is already included when an entity “Permits only necessary inbound and outbound electronic access as determined by the Responsible Entity.” If using the word “remote” is deemed necessary, the Standards Drafting Team should provide some clarity as it is not very clear what “remote” electronic access is. We feel that “remote” is already covered by Section 3.1.1.i: “between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);” The same comment applies to Sections 3.1.2 and 3.1.3 as it is not clear how using the word “remote” clarifies anything. Additionally, we believe the language in the Standards Authorization Request is proposing more strict controls/requirements for low impact BCS than the controls/requirements currently being proposed for high impact BCS and medium impact BCS in CIP-005-8 Requirements R2.1 - 2.4, and CIP-007-7 Requirement R1.1.

Likes 0	
Dislikes 0	

Response
Change made. The SDT removed the term “remote” from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1. No change. The SDT notes that the required cyber security program for lows is not stricter than the required program for mediums w/o ERC. Medium impact BCS are subject to all relevant cyber security requirements in CIP-003 through CIP-013, whereas low impact systems are only subject to the requirements in CIP-003, which are not down to individual cyber systems’ level. Medium impact BCS w/o ERC have a reduced remote access attack surface, yet still have more requirements on the individual cyber systems throughout the CIP standards. The SDT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums.

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

Document Name	
Comment	

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR; these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authentical and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect **BES Cyber System network** authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.16 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	

Dislikes 0	

Response
Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can "utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s)." The SDT changed 3.1.3 so that authentication can occur for a "network(s)" meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the "asset containing" or the authentication source used in 3.1.3 (such as an Intermediate System). Change made. The SDT has reviewed your comments and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access.

Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	No
Document Name	

Comment
We support NPCC RSC Comments

Likes 0	
Dislikes 0	

Response
See NPCC RSC response.

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1

Answer	No
Document Name	
Comment	
Section 3.1, specifically 3.1.3, is limited to the means of authentication that can be used. The standard needs to allow for a LIBCS Intermediate System equivalent. If a person could authenticate to the LIBCS Intermediate System, then remote access could be permitted from it to the Cyber Assets at the Low Impact Asset. Not all field devices support authentication, and this would help provide a means of authentication before connecting. PNMR also supports EEI's comments pertaining to Section 3, parts 3.1.4 and 3.1.6.	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can "utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s)." The SDT changed 3.1.3 so that authentication can occur for a "network(s)" meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the "asset containing" or the authentication source used in 3.1.3 (such as an Intermediate System). See EEI response.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	

ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	
AZPS does not agree with proposed language in Attachment 1 Section 3.1.4 and 3.1.6, for the other sections AZPS agrees. AZPS supports the comments and recommendations made on behalf of EEI to clarify sections 3.1.4 and 3.1.6. to ensure existing protections involving an Intermediate System meeting CIP-005-7 requirements can be utilized where applicable and protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems if using public communication links.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	No

Document Name	
Comment	
No NCPA agrees with several other comments that the proposed language places a high level of burden on entities to protect low impact assets. 3.1.2 – Would greatly increase the demand to implement and maintain a IDS type deployment and continuously update and monitor such traffic 3.1.3 – The phrase “each instances” is not well defined and does not appear anywhere else in the standards. 3.1.4 – This language requires a higher level of security than High/Med assets 3.1.6 – Needs clarification of when to disable vendor remote access	
Likes 0	
Dislikes 0	
Response	
For 3.1.2, the revisions to CIP-003-9 were made based on the scope of the approved SAR, and the DT appreciates that there may be cost associated with the implementation of the new standard. Change made. Revised to “each user-initiated instance”. The SDT notes that the required cyber security program for lows is not stricter than the required program for mediums w/o ERC. Medium impact BCS are subject to all relevant cyber security requirements in CIP-003 through CIP-013, whereas low impact systems are only subject to the requirements in CIP-003, which are not down to individual cyber systems’ level. Medium impact BCS w/o ERC have a reduced remote access attack surface, yet still have more requirements on the individual cyber systems throughout the CIP standards. The SDT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area	

than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums. 3.1.6. Change made. The SDT has reviewed your comments and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) requests additional clarity from the SDT on the intent of section 3.1 iii in the Electronic Access Controls section in which the phrase “time-sensitive communications” is referenced. CEHE believes that the language, while being overtly prescriptive, is also vague and does not entirely explain which time-sensitive protocols are being referenced. CEHE would like to request a better explanation of the inferred time-sensitive protocols included in this section.	
Likes 0	
Dislikes 0	
Response	
No change. Please see the definition for Protection Systems, which gives more context for time-sensitive “communications”. Also refer to CIP-003-8 Technical Rationale/GTB.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	

Comment	
WEC Energy Group supports and incorporates by reference the comments of the MRO (NSRF) Group for Question 1.	
Likes 0	
Dislikes 0	
Response	
See MRO NSRF response.	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	

Terminology used within 3.1 doesn't distinguish existing "electronic access" from the new term "electronic remote access." The use of the terminology "electronic remote access" generally refers to interactive remote access. Using the terminology "electronic remote access" for 3.1.1 and 3.1.2 will cause confusion.

Suggest changing 3.1.1 and 3.1.2 by deleting the word "remote" as follows:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic access; …

If the SDT retains the word "remote", the SDT should consider defining "electronic remote access" or alternatively revising "Interactive Remote Access" by adding the following statement to the existing definition of "Interactive Remove Access": **Interactive Remote Access includes remote access between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s).** The revised definition would read as follows and should be used in place of "electronic remote access".

Proposed Revision of Interactive Remote Access: User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). **Interactive Remote Access includes remote access between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s).** Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT removed the term "remote" from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	

NST respectfully offers the following observations and recommendations:

We suggest revising 3.1.4 "Protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems" to say, "Protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems from unauthorized disclosure." Given the fact the Technical Rationale document states explicitly the purpose of this requirement is to protect the confidentiality of user authentication data, we believe the requirement itself should also make this explicit.

Regarding requirements 3.1.5 and 3.1.6 (determining and disabling vendor remote access, respectively, NST notes that although the Technical Rational states the SDT's objective is to "maintain the original language used in CIP-003-9" Sections 6.1 and 6.2, this has not been done. As a presumably unintended result, the current wording of 3.1.6 ("Disable vendor electronic remote access, where vendor electronic remote access is permitted"), if interpreted literally, would require an entity to block all vendor remote access. We recommend addressing this problem by using CIP-003-9's existing language for determining and disabling vendor remote access.

Regarding the SDT's decision to merge CIP-003-9 Sections 3 and 6, NST disagrees with the SDT's assertion, "Section 6 has not been implemented or required by industry at this time and therefore there would be no impact to merging it with Section 3." While this is presently true, Registered Entities will be obliged to address requirements in Section 6 on 4/1/2026, which we expect will be at least a year before a newer version of CIP-003 that incorporates this project's changes becomes effective. We therefore believe it would be less disruptive to only move malicious communications detection from Section 6 to Section 3, leaving the other two vendor remote access requirements unchanged.

Likes 0	
Dislikes 0	

Response

Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System).

Change made. The SDT has reviewed your comments and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access.

Regarding the Implementation Plan, see implementation plan section for response.

Kimberly Turco - Constellation - 6	
Answer	No
Document Name	

Comment

To accommodate those systems that do not have the capability to perform the required function, such as protecting user authentication information in transit, Constellation recommends including language in Attachment 1, Section 3, such as "per system capability," as found throughout the rest of the CIP Standards. Specifically, Tacoma Power recommends adding the "per system capability" to the lead into Section 3 of Attachment 1. Suggested lead in language update: "Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, to mitigate risks associated with electronic access, the Responsible Entity shall implement controls, per system capability, to:"

Kimberly Turco on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

The SDT has not included “per system capability” within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the “networks containing” or “asset containing level”. The SDT also clarified the Section 3 language to also incorporate “Intermediate System” style implementations as well.

See Tacoma Power response.	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI's comments.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
NV Energy supports the comments from MRO NSRF and EEI as they relate to 3.1.4.	
Likes 0	
Dislikes 0	
Response	
See MRO NSRF and EEI response.	

David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren supports EEI's comments on this question.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No

Document Name	
Comment	

The modification to 3.1 iii is more limiting than intended. There are time-sensitive communications protocols that are unrelated to Protection Systems.

The modification to 3.1 iii could benefit from further clarification to ensure it aligns with the intended purpose and ensure industry is clear on the potential impact of this change.

Regarding 3.1.1, it would be helpful to have a clearer explanation in the Technical Rationale (TR)for changing the language to "permitting only necessary inbound/outbound REMOTE access." The objective of the TR to “maintain the original language” could be addressed more effectively by the SDT.

Although 3.1.2 exceeds the Standards for Medium Impact and incurs substantial costs. The challenge lies in the fact these terms have acquired specific connotations, such as those associated with medium/high controls centers. Consequently, their reuse should be restricted, and any lesser measures, such as monitoring firewall logs, should not be authorized.

The prescriptiveness of 3.1.3 seems to go beyond what is typically expected for Medium Impact.

Similarly, 3.1.4 appears to exceed the standards for Medium Impact. It would be helpful to revisit this requirement as well.

With regards to 3.1.5 and 3.1.6, the change from "have methods" to "implement controls to" introduces some ambiguity and alters the previously approved requirements. Implementing a control to determine vendor electronic remote access seems very different than having methods for determining vendor electronic remote access. The technical rationale suggests that the SDT intends to uphold the initial language, despite having, in reality, modified the language.

Likes 0	
Dislikes 0	

Response

1. No change. This revision was updated based on CIP-003-10 version from Project 2016-02, which was approved by industry ballot.

2. Change made. The SDT removed the term “remote” from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1.
3. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System).
4. Change made. The SDT has reviewed your comments and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access.

Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	

Comment

The modification to 3.1 iii is more limiting than intended. There are time-sensitive communications protocols that are unrelated to Protection Systems.

The modification to 3.1 iii could benefit from further clarification to ensure it aligns with the intended purpose and ensure industry is clear on the potential impact of this change.

Regarding 3.1.1, it would be helpful to have a clearer explanation in the Technical Rationale (TR)for changing the language to "permitting only necessary inbound/outbound REMOTE access." The objective of the TR to “maintain the original language” could be addressed more effectively by the SDT.

Although 3.1.2 exceeds the Standards for Medium Impact and incurs substantial costs. The challenge lies in the fact these terms have acquired specific connotations, such as those associated with medium/high controls centers. Consequently, their reuse should be restricted, and any lesser measures, such as monitoring firewall logs, should not be authorized.

The prescriptiveness of 3.1.3 seems to go beyond what is typically expected for Medium Impact. Similarly, 3.1.4 appears to exceed the standards for Medium Impact. It would be helpful to revisit this requirement as well. With regards to 3.1.5 and 3.1.6, the change from "have methods" to "implement controls to" introduces some ambiguity and alters the previously approved requirements. Implementing a control to determine vendor electronic remote access seems very different than having methods for determining vendor electronic remote access. The technical rationale suggests that the SDT intends to uphold the initial language, despite having, in reality, modified the language.	
Likes 0	
Dislikes 0	
Response	
See response above.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	No
Document Name	
Comment	
ACES feels, “Section 3.1.4 Protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems”, should read: Protect electronic remote access information in transit to or from the asset containing low impact BES Cyber Systems;” The addition of authentication of remote users we are fine with, but the SDT chose to just scope in protection of remote user authentication information and we feel that is not the only thing that should be protected. Just like in the case of detection of vendor communication versus all communications (fixed in this version), we feel ALL electronic remote access information should be protected just as it is in CIP-005 R2 if it’s FERC/NERC’s intention of reducing overall cybersecurity risk with this change. Without fully protecting the entire remote access session, risks are only minimally reduced and this standard will have to be revised again to meet the objective.	
Likes 0	

Dislikes 0	

Response

No change. Thank you for the comment. The SDT intent was to stay within the scope outlined in the SAR and the LICRT Report, both of which specifically mention user authentication information.

Alison MacKellar - Constellation - 5

Answer	No
Document Name	

Comment

To accommodate those systems that do not have the capability to perform the required function, such as protecting user authentication information in transit, Constellation recommends including language in Attachment 1, Section 3, such as "per system capability," as found throughout the rest of the CIP Standards. Specifically, Tacoma Power recommends adding the "per system capability" to the lead into Section 3 of Attachment 1. Suggested lead in language update: "Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, to mitigate risks associated with electronic access, the Responsible Entity shall implement controls, per system capability, to:"

Alison Mackellar on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

The SDT has not included “per system capability” within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the “networks containing” or “asset containing level”. The SDT also clarified the Section 3 language to also incorporate “Intermediate System” style implementations as well.

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments. Please clarify whether vendor electronic remote access includes cases involving protocol transition between serial and TCP/IP.	
Likes 0	
Dislikes 0	
Response	
See NPCC RSC response.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports the comments of MRO NSRF and EEI.	
Likes 0	
Dislikes 0	
Response	
See MRO NSRF and EEI responses.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No

Document Name	
Comment	
Texas RE agrees with the proposed language in Sections 3.1.2, 3.1.3, 3.1.4, 3.1.5, and 3.1.6. Texas is concerned, however, with the term electronic remote access in Section 3.1. This phrase changes the scope of the requirement to potentially no longer include communications that are not used for remote access. For example, the proposed addition of "remote" could arguably exclude Domain Name System (DNS) and ping queries from the scope of the CIP-003 protections, potentially allowing unnecessary electronic access using these types of traffic. Such traffic has been associated with malicious attacks, including DNS cache poisoning and other activities that are not exclusively linked to remote access. As such, there is a potential reliability gap if this language is retained. Texas RE recommends removing the word “remote” in Section 3.1.1.	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT removed the term “remote” from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1. Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tracy MacNicoll - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
The proposed language of Section 3 has lists within lists. This makes it difficult to understand how the items in each list apply to each other. The roman numerals i-iii apply to 3.1.1.-3.1.6. but this may be misinterpreted in future CMEP engagements. This also causes the standard to deviate from what is understood to be the NERC style “and/or” lists. As proposed, 3.1 and 3.2 are the list items for the Section 3 language “Responsible Entity shall implement controls to:”. Since 3.1 and 3.2 are the two items in a list, 3.1 should end with the word “and” to differentiate it from an “or” list. Propose the following changing “…the Responsible Entity shall implement controls to:” to “…the Responsible Entity shall implement the following controls.”	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.	

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the proposed language in CIP-003-A Attachment 1.	
Likes 1	Corn Belt Power Cooperative, 1, brusseau Larry
Dislikes 0	
Response	

Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	

Although we can agree with the proposed changes, we have a suggested change to Attachment 1, Section 3.1.3 in the event another draft is necessary:

The currently proposed langage is "Authenticate users when permitting each instance of electronic remote access to networks containing low impact BES Cyber Systems;".

MRO suggests using language more similar to the definition of Interactive Remote Access (IRA). IRA is defined as “user-initiated access by a person a remote access client or other remote access technology…”. Considering that, MRO suggests inserting "user-initiated" following the word "each" on that proposed language, which would result in "Authenticate users when permitting each **user-initiated** instance of electronic remote access to networks containing low impact BES Cyber Systems;".

Without such a change, the proposed language can be interpreted as introducing system-to-system communications into the equation, which we don't believe was intended.	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System).	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steve Toosevich - Steve Toosevich, Group Name NIPSCO Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy – Duke Energy	
Answer	Yes
Document Name	
Comment	
We support the revisions as posted but do support the alternative language recommendations from EEI for 3.1.4 and 3.1.6 for further clarity.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	

2. Do you agree with the language proposed in CIP-003-A Attachment 2? If you do not agree, please provide recommended language you would support and, if appropriate, technical or procedural justification.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports the comments of MRO NSRF and EEI.	
Likes 0	
Dislikes 0	
Response	
See MRO NSRF and EEI responses.	
Alison MacKellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation recommends changing CIP-003-A, Attachment 2, in conformance with our comments to Question 1. Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	

See SDT response to Constellation comments in Question 1.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
We do not concur with the proposed language in Attachment 2 for the same reasons we do not agree with the language in Attachment 1. Please see the response to question 1 above.	
Likes 0	
Dislikes 0	
Response	
See SDT response to Georgia Transmission Corporation comments in Question 1. Additionally, the SDT made conforming changes to Attachment 2 based on new revisions made to Attachment 1. The intent of these revisions was to clarify what type of electronic access was in scope and add more examples of evidence that may be conducive for other network configurations, such as those where Responsible Entities use an Intermediate System(s) to facilitate user-initiated instances of electronic access to multiple BES Cyber Systems with varying impact levels.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
We do not concur with the proposed language in Attachment 2 for the same reasons we do not agree with the language in Attachment 1. Please see the response to question 1 above.	
Likes 0	
Dislikes 0	

Response	
See SDT response to Georgia System Operations Corporation comments in Question 1. Additionally, the SDT made conforming changes to Attachment 2 based on new revisions made to Attachment 1. The intent of these revisions was to clarify what type of electronic access was in scope and add more examples of evidence that may be conducive for other network configurations, such as those where Responsible Entities use an Intermediate System(s) to facilitate user-initiated instances of electronic access to multiple BES Cyber Systems with varying impact levels.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren supports EEI's comments on this question.	
Likes 0	
Dislikes 0	

Response	
See EEI response.	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI's comments.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
Constellation recommends changing CIP-003-A, Attachment 2, in conformance with our comments to Question 1. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	

See SDT's response to above Constellation comments in question 2.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
As per our response to Question 1, NST recommends leaving requirements for detecting and disabling vendor remote access in Section 6, moving only malicious communications detection to Section 3.	
Likes 0	
Dislikes 0	
Response	
See SDT response to NST comments in Question 1.	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
Terminology used within Section 3. does not distinguish existing "electronic access" from the new term "electronic remote access." The use of the terminology "electronic remote access" generally refers to interactive remote access. Using the terminology "electronic remote access" for Section 3. Item 1 may cause confusion. SDT should consider defining "electronic remote access" or redefining "Interactive Remote Access" as follows and using that in place of "electronic remote access."	

Continent-wide Term

Interactive Remote Access

Definition

User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Interactive Remote Access includes remote access between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

Suggest changing Section 3. Item 1 as follows:

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation For Section 3.1.1, documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive these communications are time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative Protection Systems, such as:

Suggest changing Section 3. Item 5 as follows for consistency: "5. For Section 3.1.5 documentation showing the ability to determine vendor electronic remote access, such as…"	
Likes 0	
Dislikes 0	
Response	
See SDT response to Southern Indiana Gas and Electric Co. comments in Question 1.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	
WEC Energy Group supports and incorporates by reference the comments of the MRO (NSRF) Group for Question 2.	
Likes 0	
Dislikes 0	
Response	
See MRO NSRF response.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	

Terminology used within Section 3. does not distinguish existing “electronic access” from the new term “electronic remote access.” The use of the terminology “electronic remote access” generally refers to interactive remote access. Using the terminology “electronic remote access” for Section 3. Item 1 may cause confusion.

SDT should consider defining “electronic remote access” or redefining “Interactive Remote Access” as follows and using that in place of “electronic remote access.”

Continent-wide Term

Interactive Remote Access

Definition

User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity’s Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Interactive Remote Access includes remote access between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

Suggest changing Section 3. Item 1 as follows:

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation For Section 3.1.1, documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive these communications are time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative Protection Systems, such as:

Suggest changing Section 3. Item 5 as follows for consistency: "5. For Section 3.1.5 documentation showing the ability to determine vendor electronic remote access, such as..."	
Likes 0	
Dislikes 0	
Response	
See SDT response to CenterPoint Energy comments in Question 1.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	No
Document Name	
Comment	
No NCPA agrees with several other comments that the proposed language places a high level of burden on entities to protect low impact assets. 3.1.2 – Would greatly increase the demand to implement and maintain a IDS type deployment and continuously update and monitor such traffic 3.1.3 – The phrase “each instances” is not well defined and does not appear anywhere else in the standards. 3.1.4 – This language requires a higher level of security than High/Med assets 3.1.6 – Needs clarification of when to disable vendor remote access	

Likes 0	
Dislikes 0	
Response	
See SDT's response to NCPA comments in question 1.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	
AZPS does not agree with the proposed language in Attachment 2. AZPS supports EEI's recommendation to add an option that would permit protection of user authentication information in transit between the user and the intermediate system, and not just the asset containing low impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	

Response	
See EEI response.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI does not support the proposed language changes to Attachment 2 and propose adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the asset containing low impact BES Cyber Systems. (See EEI's comments and proposed changes as provided in our response to question 1)	
Likes 0	
Dislikes 0	
Response	
The SDT made conforming changes to Attachment 2 based on new revisions made to Attachment 1. The intent of these revisions was to clarify what type of electronic access was in scope and add more examples of evidence that may be conducive for other network configurations, such as those where Responsible Entities use an Intermediate System(s) to facilitate user-initiated electronic access to multiple BES Cyber Systems with varying impact levels.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	

We feel that using the words “outbound electronic remote access” in Section 3 is confusing and we do not think adding the word “remote” so that the language states “… inbound and outbound electronic “remote” access…” clarifies anything. We recommend striking the word “remote”.	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT removed the term “remote” from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
Please refer to LCRA’s concerns in question 1.	
Likes 0	
Dislikes 0	
Response	
See SDT’s response to LCRA comments in question 1.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	

Please refer to LCRA's concerns in question 1.	
Likes 0	
Dislikes 0	
Response	
See SDT's response to LCRA comments in question 1.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is in support of EEIs response to this question.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	

Dislikes 0	
Response	
See EEI response.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
For CIP-003-A Requirement R2 Attachment 2, Section 3, Requirement Part 3.1.4, NSRF requests further SDT consideration of an adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the the asset containing low impact BES Cyber Systems.	
Likes 1	Corn Belt Power Cooperative, 1, brusseau Larry
Dislikes 0	
Response	
The SDT made conforming changes to Attachment 2 based on new revisions made to Attachment 1. The intent of these revisions was to clarify what type of electronic access was in scope and add more examples of evidence that may be conducive for other network configurations, such as those where Responsible Entities use an Intermediate System(s) to facilitate user-initiated electronic access to multiple BES Cyber Systems with varying impact levels.	
Ben Hammer - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
see question 1 comments, attachment 2 should be rewritten to cover the appropriate changes based off the comments on question 1.	

Likes 0	
Dislikes 0	
Response	
See SDT's response to WAPA comments in question 1. Additionally, the SDT made conforming changes to Attachment 2 based on new revisions made to Attachment 1.	
Josh Combs - Black Hills Corporation - 3	
Answer	No
Document Name	
Comment	
Black Hills Corporation agrees with EEI's comments: we do not support the proposed language changes to Attachment 2 and propose adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the asset containing low impact BES Cyber Systems. (See EEI's proposed change to question 1)	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Carly Miller - Carly Miller On Behalf of: Sheila Suurmeier, Black Hills Corporation, 5, 6, 1, 3; - Carly Miller	
Answer	No
Document Name	
Comment	

Black Hills Corporation agrees with EEI's comments: we do not support the proposed language changes to Attachment 2 and propose adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the asset containing low impact BES Cyber Systems. (See EEI's proposed change to question 1)	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Micah Runner - Black Hills Corporation - 1	
Answer	No
Document Name	
Comment	
Black Hills Corporation agrees with EEI's comments: we do not support the proposed language changes to Attachment 2 and propose adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the asset containing low impact BES Cyber Systems. (See EEI's proposed change to question 1)	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	No
Document Name	
Comment	

Black Hills Corporation agrees with EEI's comments: we do not support the proposed language changes to Attachment 2 and propose adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the asset containing low impact BES Cyber Systems. (See EEI's proposed change to question 1)	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
EEI does not support the proposed language changes to Attachment 2 and propose adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the asset containing low impact BES Cyber Systems. (See EEI's proposed change to question 1)	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Tracy MacNicoll - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	

The examples of evidence for R3.1.1 should also include the documentation of why the communication is needed since the entity is required for low impact assets to implement the controls based on their need.	
Likes 0	
Dislikes 0	
Response	
The SDT believes this request is outside the current SAR and is a compliance interpretation. No change has been made.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

1. Section 3.1.2 creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers: the proposed language requires detection of known/suspected malicious communications for "inbound and outbound electronic remote access." There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5).

BPA suggests that this requirement be removed for better consistency with the requirements for Medium BCS.

2. Section 3.1.4 creates a higher compliance bar for Low BCS than for Medium BCS: in the latest Draft 5 of CIP-005-8 R2.2 - 2.3, the proposed requirements include only Interactive Remote Access, or human-initiated access. Section 3.1.4 includes all "information in transit to or from the asset containing low impact BES Cyber Systems."

BPA suggests that this requirement be aligned with the latest Draft 5 of CIP-005-8 R2.2 - 2.3: "3.1.4 Protect user authentication *of IRA communications* in transit to or from the asset containing low impact BES Cyber Systems."

3. Section 3.1.6: While BPA appreciates the committee's intent to "present a single section for all electronic access" (Technical Rationale, p. 2), Section 3.1.6 is nonetheless awkwardly worded. It either suggests that all vendor remote access should be disabled

(rather than requiring controls that could provide an option to disable vendor remote access), or it contradicts itself in a nonsensical sentence by saying that when vendor access is permitted, it should always be disabled. BPA suggests aligning with the language used in Draft 5 of CIP-003-10, such as "Have one or more methods" for determining and disabling vendor remote access sessions.	
Likes 0	
Dislikes 0	
Response	
See SDT's response to BPA comments in question 1.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
SRP agrees and supports Tacoma Power's comment to incorporate the proposed changes outlined in Q1.	
Likes 0	
Dislikes 0	
Response	
See SDT's response to Tacoma Power comments in question 1.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

Per answer in question #1.	
Likes 0	
Dislikes 0	
Response	
See SDT's response to Tri-State G and T Association, Inc. comments in question 1.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
The language in 3.1.2 is specifying an IDS/IPS which depending on the capability of cyber assets at the low impact assets, could be infeasible or cost prohibitive to implement/replace equipment and should take into account that many cyber assets could be limited in their ability to communicate with monitoring/detection systems, communication protocols, etc. Also, in 3.1.4, the SDT should consider modifying language that focuses on mitigating risks to protect user authentication information and allow entities to determine their methods to mitigate risks that fit with their current network configuration(s). The SDT should also consider adding "per Cyber System/Asset capability" to address this reality that many cyber assets have limitations and may not be easily upgraded or replaced.	
Likes 0	
Dislikes 0	
Response	
For 3.1.2, the revisions were made based on the scope of the approved SAR, and the SDT appreciates that there may be cost associated with the implementation of the new standard. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the "asset containing" or the authentication source used in 3.1.3 (such as an Intermediate System).	

The SDT has not included “per system capability” within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the “networks containing” or “asset containing level”. The SDT also clarified the Section 3 language to also incorporate “Intermediate System” style implementations as well.	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	No
Document Name	
Comment	
Eversource agrees with the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
See comments to Q1.	
Likes 0	
Dislikes 0	
Response	
See SDT’s response to Dominion comments in question 1.	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Tacoma Power recommends changing CIP-003-A, Attachment 2, in conformance with our comments to Question 1.	
Likes 1	LaKenya Vannorman, N/A, Vannorman LaKenya
Dislikes 0	
Response	
Change Made. The SDT made conforming changes to Attachment 2 based on new revisions made to Attachment 1.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The number of Low Impact BES Cyber Systems impacted would make achieving compliance burdensome in terms of level of effort, cost, and required technology implementations.	
Likes 0	
Dislikes 0	
Response	
The revisions were made based on the scope of the approved SAR, and the SDT appreciates that there may be effort and cost associated with the implementation of the new standard.	

Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute for question #2.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
Based on concerns about Attachment 1 listed above this section requires adjustment.	
Likes 0	
Dislikes 0	
Response	
See SDT's response to FirstEnergy comments in question 1. Additionally, the SDT made conforming changes to Attachment 2 based on new revisions made to Attachment 1.	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF requests the SDT to review the proposed language in CIP-003-A Attachment 2, Section 3, Part 1 stating “except where these communications are time-sensitive protection or control functions between Protection Systems,” and compare it to the proposed language in Attachment 1, Section 3.1.iii “not used for time-sensitive communications of Protection Systems.” to ensure consistency.	
Likes 0	
Dislikes 0	
Response	
To maintain consistency with the electronic access defined within Section 3.1 of Attachment 1, the SDT modified the language to “where electronic access meets the criteria specified in Section 3.1”.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
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 Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Steve Toosevich - Steve Toosevich, Group Name NIPSCO Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE noticed the formatting of Attachment 2, Section 3 is not consistent with Attachment 1. Texas RE recommends it contain subsections 3.1 – 3.7. Texas RE is similarly concerned with the addition of "remote" in the phrase electronic remote access as in Attachment 1. Texas RE recommends removing the term "remote" from Section 3, #1.	
Likes 0	
Dislikes 0	
Response	
The SDT did not restructure Section 3 of Attachment 2, however, the SDT agrees that the way the section was structured in Section 3 of Attachment 1 modifications would be needed. The SDT believes that the adjustments made to Section 3 of Attachment 1 and the conforming changes made to Section 3 of Attachment 2, fixed the consistency aspect that was previously questionable. The SDT removed the term "remote" from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1.	
Ellese Murphy – Duke Energy	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	

3. The Standard Drafting Team (SDT) proposes a three (3) year implementation plan for CIP-003-A. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with detailed explanation.

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

Answer	No
Document Name	

Comment

If this standard were to be drafted as-is, large organizations would be compelled to implement substanial technological changes on a grand scale, including significant cost capital and O&M increases which would need to be accounted for on an ongoing basis as well as marshalling of significant contracted labor to execute this massive directive. Consider a tier-ed based approach based on certain risk-based factors, existing connectivity types, capabilities, etc.

FirstEnergy also supports EEI's comments which state:

The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to

Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see EEI response for question 3.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The number of Low Impact BES Cyber Systems impacted would make achieving compliance burdensome in terms of level of effort, cost, and required technology implementations within the implementation timeframe.	
Likes 0	
Dislikes 0	
Response	
No change. The revisions to CIP-003-9 were made based on the scope of the approved SAR, and the SDT appreciates that there may be cost associated with the implementation of the new standard.	
Steve Toosevich - Steve Toosevich, Group Name NIPSCO Compliance	
Answer	No
Document Name	

Comment	
Responsible entities are currently ensuring compliance with CIP-003-8 and preparation for the approved CIP-003-9. The three (3) year implementation plan of CIP-003-A would quickly follow the changes implemented in CIP-003-9 while anticipating modifications to the Standards for Project 2016-02 Modifications to CIP Standards.	
Likes 0	
Dislikes 0	
Response	
No change. The cybersecurity controls proposed for CIP-003-A do not conflict with and build upon the requirements for CIP-003-9 for vendor remote access for those with vendor access controls, while also meeting the requirements of the approved SAR for this project.	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	No
Document Name	
Comment	
Eversource agrees with the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response for question 3.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No

Document Name	
Comment	
With the restrictive and prescriptive language as currently proposed, those Responsible Entities with a significant number of low impact assets containing low impact BCS could find it impossible to implement a solution in 3 years. The SDT should consider adding "per Cyber System/Asset capability" to address the reality that many cyber assets have limitations and would require a large effort to replace and implement new cyber assets; and this does not begin to address the potential for equipment supply chain issues and delivery lead times which have not returned to normal for equipment purchases.	
Likes 0	
Dislikes 0	
Response	
Please see response to Questions 1 & 2. The SDT has not included "per system capability" within Section 3 since the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the "networks containing" or "asset containing" level. The SDT clarified the Section 3 language to also incorporate "Intermediate System" style implementations as well.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
If specific date of implementation is defined, SRP might agree. There is significant cost (equipment and resources), time for planning, and work will need to be done.	
Likes 0	
Dislikes 0	

Response	
For US entities, the proposed effective date is 36 months (3 years) after FERC approval date.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Until Questions 1 and 2 are resolved it is difficult for BPA to determine if the 3 year timeframe is appropriate.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see responses to questions 1 and 2.	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.	

Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	No
Document Name	
Comment	
Black Hills Corporation agrees with the comments provided by EEI. The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	
Micah Runner - Black Hills Corporation - 1	
Answer	No
Document Name	
Comment	

Black Hills Corporation agrees with the comments provided by EEI. The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	
Carly Miller - Carly Miller On Behalf of: Sheila Suurmeier, Black Hills Corporation, 5, 6, 1, 3; - Carly Miller	
Answer	No
Document Name	
Comment	
Black Hills Corporation agrees with the comments provided by EEI. The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	

Josh Combs - Black Hills Corporation - 3	
Answer	No
Document Name	
Comment	
Black Hills Corporation agrees with the comments provided by EEI. The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
The absence of per Cyber System capability in CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4 may create an impossibility to comply within the implementation timeline without wholesale upgrades or replacements of technology and communications infrastructure. NSRF requests further SDT consideration of the addition of "*per Cyber System capability*" language in CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4.	

Likes 1	Corn Belt Power Cooperative, 1, brusseau Larry
Dislikes 0	

Response
No change. The SDT has not included “per system capability” within Section 3 since the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the “networks containing” or “asset containing level”. The SDT also clarified the Section 3 language to incorporate “Intermediate System” style implementations as well.

Daniel Gacek - Exelon - 1	
Answer	No
Document Name	

Comment
Exelon supports the comments submitted by the EEI.

Likes 0	
Dislikes 0	

Response
Thank you for the comment, please see EEI response.

Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	

Comment
Exelon is in support of EEIs response to this question.

Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
LCRA believes that a 3-year implementation plan may not be sufficient due to the sheer number of Low Impact BES Cyber Systems. Additionally, there is considerable unknowns regarding the new requirements. Please see LCRA's response to question 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment. Please see the response to LCRA Question 1 comments.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
LCRA believes that a 3-year implementation plan may not be sufficient due to the sheer number of Low Impact BES Cyber Systems. Additionally, there is considerable unknowns regarding the new requirements. Please see LCRA's response to question 1.	
Likes 0	

Dislikes 0	
Response	
Thank you for the comment. Please see the response to LCRA Question 1 comments.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. No change. The proposed implementation plan timeline is thirty-six (36) months after the effective date, which takes into account the April 1, 2026 effective date of CIP-003-9. The proposed changes to the implementation timeline of CIP-003-10 are outside the purview of this project; however, the SDT is aware of the 2016-02 revisions in CIP-003-10. The SDT notes that since 2016-02 has yet to complete final ballot, receive Board of Trustees approval, and be filed with and approved by FERC, it is not possible to know what the final effective date of CIP-003-10 will be.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	

Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	
AZPS does not agree with the proposed implementation plan. AZPS agrees with EEI's comments that the 3 year implementation plan would be acceptable if there were not other industry standards projects underway that will also require changes affecting low impact BCS with differing deadlines.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	

Comment
The pending changes for CIP-003 in other NERC projects would equate to implementing changes that would, within a relatively short time, be modified and be subject to further modifications. Additionally, CEHE supports the included EEI comments that address timing and pending NERC projects. EEI Comment: The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.

Likes 0	
Dislikes 0	

Response
Thank you for the comment, please see EEI response.

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	

Comment
WEC Energy Group supports and incorporates by reference the comments of the MRO (NSRF) Group for Question 3.

Likes 0	
Dislikes 0	

Response	
Thank you for the comment, please see MRO Group response.	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren supports EEI's comments on this question.	
Likes 0	
Dislikes 0	
Response	

Thank you for the comment, please see EEI response.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
We do not agree with the proposed implementation plan. Our apprehension primarily stems from the intersection of CIP-003-A and CIP-003-9, with a particular focus on the potential financial implications in Section 6.3, where additional expenditures may be necessitated to accommodate technological changes.	
Likes 0	
Dislikes 0	
Response	

No change. The SDT appreciates that there may be costs associated with implementing these changes.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
We do not agree with the proposed implementation plan. Our apprehension primarily stems from the intersection of CIP-003-A and CIP-003-9, with a particular focus on the potential financial implications in Section 6.3, where additional expentitures may be necessitated to accommodate technological changes.	
Likes 0	
Dislikes 0	
Response	
No change. The SDT appreciates that there may be costs associated with implementing these changes.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports the comments of MRO NSRF and EEI.	
Likes 0	
Dislikes 0	
Response	

Thank you for the comment, please see MRO Group and EEI responses.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the proposed 3-year implementation plan.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes

Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 1	LaKenya Vannorman, N/A, Vannorman LaKenya
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Tracy MacNicoll - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1,3	

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 Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
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	
Ellese Murphy – Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

4. The SDT believes the language of CIP-003-A addresses the issues outlined in the SAR in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports the comments of MRO NSRF and EEI.	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	

3.1.2 exceeds the Standards for Medium Impact and incurs substantial costs. The challenge lies in the fact these terms have acquired specific connotations, such as those associated with medium/high controls centers. Consequently, their reuse should be restricted, and any lesser measures, such as monitoring firewall logs, should not be authorized	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

3.1.2 exceeds the Standards for Medium Impact and incurs substantial costs. The challenge lies in the fact these terms have acquired specific connotations, such as those associated with medium/high controls centers. Consequently, their reuse should be restricted, and any lesser measures, such as monitoring firewall logs, should not be authorized.	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
Further analysis is needed to determine if the benefits outweigh the cost of additional equipment needing to be purchased in order to achieve compliance.	

Likes 0	
Dislikes 0	

Response

The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency.

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group

Answer	No
Document Name	

Comment

WEC Energy Group supports and incorporates by reference the comments of the MRO (NSRF) Group for Question 4.

Likes 0	
Dislikes 0	

Response

The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency.

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	No
Document Name	
Comment	
No NCPA agrees with several other comments that the proposed language places a high level of burden on entities to protect low impact assets. 3.1.2 – Would greatly increase the demand to implement and maintain a IDS type deployment and continuously update and monitor such traffic 3.1.3 – The phrase “each instances” is not well defined and does not appear anywhere else in the standards. 3.1.4 – This language requires a higher level of security than High/Med assets 3.1.6 – Needs clarification of when to disable vendor remote access	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally,	

the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. The SDT has not included “per system capability” within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the “networks containing” or “asset containing level”. The SDT also clarified the Section 3 language to also incorporate “Intermediate System” style implementations as well. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System). 3.1.5 and 3.1.6. Change made. The SDT has reviewed your comments and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access. Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.

Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	

AZPS does not agree the changes are cost effective as these would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS.	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. The SDT notes that the required cyber security program for lows is not stricter than the required program for mediums w/o ERC. Medium impact BCS are subject to all relevant cyber security requirements in CIP-003 through CIP-013, whereas low impact systems are only subject to the requirements in CIP-003, which are not down to individual cyber systems’ level. Medium impact BCS w/o ERC have a reduced remote access attack surface, yet still have more requirements on the individual cyber systems throughout the CIP standards. The SDT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums.	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	
Answer	No
Document Name	
Comment	

PNMR sees potential excessive costs in implementing 3.1.4 – particularly if the need arose to install a substation server at each LIBCS substation (as there are many field devices with varying and older protocols in place) in order to ensure the correct protocols were met.	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System).	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
LCRA cannot determine the cost effectiveness of these proposals due to the sheer number of Low Impact BES Cyber Systems. Additionally, there is considerable unknowns regarding the new requirements. Please see LCRA’s response to question 1.	
Likes 0	

Dislikes 0	

Response

The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency.

Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System).

Teresa Krabe - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

LCRA cannot determine the cost effectiveness of these proposals due to the sheer number of Low Impact BES Cyber Systems. Additionally, there is considerable unknowns regarding the new requirements. Please see LCRA’s response to question 1.

Likes 0	
Dislikes 0	

Response

The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System).	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
GO/GOPs will need more information to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally,	

the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
The absence of per Cyber System capability in CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4 may require premature wholesale upgrades or replacement of communications or operational technology that has not met its end of life in order to comply. NSRF requests further SDT consideration of the addition of "*per Cyber System capability*" language in CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4.	
Likes 1	Corn Belt Power Cooperative, 1, brusseau Larry
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a "network(s)" meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. The SDT has not included "per system capability" within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the "networks containing" or "asset containing level". The SDT also clarified the Section 3 language to also incorporate "Intermediate System" style implementations as well.	
Ben Hammer - Western Area Power Administration - 1	
Answer	No

Document Name	
Comment	
The absence of per Cyber System capability in CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4 may require premature wholesale upgrades or replacement of communications or operational technology that has not met its end of life in order to comply. NSRF requests further SDT consideration of the addition of "*per Cyber System capability*" language in CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a "network(s)" meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. The SDT has not included "per system capability" within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the "networks containing" or "asset containing level". The SDT also clarified the Section 3 language to also incorporate "Intermediate System" style implementations as well.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	

More information required. Unable to determine exact financial impact, but it is significant and needs to be allowed for in the budget.	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
Large entities with a large number of cyber assets could incur significant capital and O&M expenditures and labor costs that would be unrealistic if there is only a 3 year implementation plan. This could cause entities to make financial decisions that are not cost effective. The SDT is encouraged to consider the addition of “per Cyber System/Asset capability” and provide a more tiered approach for those entities with a significant number of cyber assets.	
Likes 0	
Dislikes 0	
Response	

The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. The SDT has not included “per system capability” within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the “networks containing” or “asset containing level”. The SDT also clarified the Section 3 language to also incorporate “Intermediate System” style implementations as well.	
Steve Toosevich - Steve Toosevich, Group Name NIPSCO Compliance	
Answer	No
Document Name	
Comment	
Responsible Entities would potentially need to purchase new equipment to meet the proposed language of the Standard.	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	

Answer	No
Document Name	
Comment	
The number of Low Impact BES Cyber Systems impacted would make achieving compliance burdensome in terms of level of effort, cost, and required technology implementations within the implementation timeframe.	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. The SDT has not included “per system capability” within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the “networks containing” or “asset containing level”. The SDT also clarified the Section 3 language to also incorporate “Intermediate System” style implementations as well. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System).	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	

Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the MRO NSRF for question #4.	
Likes 1	Corn Belt Power Cooperative, 1, brusseau Larry
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
This proposal would be prohibitively expensive both to build and operate over time. To be “cost effective” implies the proposed modification to the CIP-003 standard can be absorbed with existing company staff and minor procedure adjustment. Based on the high volume of Low Impact Cyber System locations and varied configurations that we have in our service territory (approximately 10 times the level of CIP Medium Impact locations), this is not a cost-effective change but is rather a cost-prohibitive mandate. Substantial additional funding (capital and O&M), staffing, and compliance programs will be required to meet the proposed requirements.	
Likes 0	

Dislikes 0	

Response
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. The SDT has not included “per system capability” within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the “networks containing” or “asset containing level”. The SDT also clarified the Section 3 language to also incorporate “Intermediate System” style implementations as well. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System). Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	

PNMR sees potential excessive costs in implementing 3.1.4 – particularly if the need arose to install a substation server at each LIBCS substation (as there are many field devices with varying and older protocols in place) in order to ensure the correct protocols were met.	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System). Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency.	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes

Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
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 Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	

Likes 1	LaKenya Vannorman, N/A, Vannorman LaKenya
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren has no comments on the cost effectiveness of this project.	

Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
NST is unable to assess the cost effectiveness of the proposed approaches to addressing the SAR.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	
Document Name	
Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Josh Combs - Black Hills Corporation - 3	
Answer	
Document Name	
Comment	
Black Hills Corporation will not comment on cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Carly Miller - Carly Miller On Behalf of: Sheila Suurmeier, Black Hills Corporation, 5, 6, 1, 3; - Carly Miller	
Answer	

Document Name	
Comment	
Black Hills Corporation will not comment on cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Micah Runner - Black Hills Corporation - 1	
Answer	
Document Name	
Comment	
Black Hills Corporation will not comment on cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	
Document Name	
Comment	

Black Hills Corporation will not comment on cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	
NEE does not comment on costs.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	

Dislikes 0	
Response	
Ellese Murphy – Duke Energy	
Answer	Yes
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	

5. Provide any additional comments on the standard and technical rationale for the SDT to consider, if desired.
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE
Answer
Document Name
Comment
While PNMR does agree that coordinated attacks present risk, it is unclear as to the realized risk associated with a coordinated attack utilizing multiple low-impact BES Cyber Systems. As it would be difficult to quantify the number of low-impact systems needed to be

utilized in a potential coordinated attack and with uncertain findings as to the use of low-impact systems to conduct a coordinated attack, PNM believes the potential risk to the BES from such attacks does not sufficiently correlate with the proposed authentication and detection controls which would be a vast expansion of scope. The NERC Low Impact Criteria Review Report references the risk of coordinated attacks on low impact BES Cyber Systems for those systems that are determined by the CIP-002 Standards. However, the CIP-002 categorization of BES Cyber Systems is not intended to take into account the effect of a coordinated attack in determining the categorization of a BES Cyber System. This language seems to attempt to change the purpose and muddy the scope of the CIP-002 Standard. PNMR also has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.	
Likes 0	
Dislikes 0	
Response	
The LICRT indicated they do not recommend changing the CIP-002 impact rating criteria used in identifying and categorizing individual BES Cyber Systems. Changes to CIP-002 are not included in the scope of the SAR for this project. The SDT is not authorized in the SAR to revise all of the standards. By having the low impact contained in CIP-002 and CIP-003, this allows "low impact only Entities" to comply with those two standards.	
Deanna Carlson - Cowlitz County PUD – 5	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	

Response	
Patricia Lynch - NRG - NRG Energy, Inc. – 5	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	

Answer	
Document Name	
Comment	
Nothing further to provide at this time.	
Likes 0	
Dislikes 0	
Response	

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

Answer	
Document Name	
Comment	
The language as proposed fails to clearly identify the target of the compliance objective. Suggest the SDT revise the language to clarify whether the target is the network containing the Low BCS, the Low BCS, or other Cyber Assets contained in the network. The undefined term “electronic remote access” used throughout the proposed language lacks sufficient clarity. Suggest the SDT provide a definition to be entered into the NERC Glossary to provide consistent application.	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also	

allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification. The SDT removed the term "remote" from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. – 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	
Document Name	
Comment	
SRP feels there is some concern for CIP-003 being written for low impact requirements that contain parts of all existing standards (for medium and high impact). Seems like there is an opportunity to just add low impact requirements to the existing standard(s). This will also help in keeping language consistent.	
Likes 0	
Dislikes 0	
Response	
The SDT is not authorized in the SAR to revise all of the standards. By having the low impact contained in CIP-002 and CIP-003, this allows "low impact only Entities" to comply with those two standards.	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	
Document Name	
Comment	
Black Hills Corporation agrees with PNMR and has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.	
Likes 0	
Dislikes 0	

Response	
See PNMR response. The SDT is not authorized in the SAR to revise all of the standards. By having the low impact contained in CIP-002 and CIP-003, this allows “low impact only Entities” to comply with those two standards.	
Micah Runner - Black Hills Corporation – 1	
Answer	
Document Name	
Comment	
Black Hills Corporation agrees with PNMR and has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.	
Likes 0	
Dislikes 0	
Response	
See PNMR response. The SDT is not authorized in the SAR to revise all of the standards. By having the low impact contained in CIP-002 and CIP-003, this allows “low impact only Entities” to comply with those two standards.	
Carly Miller - Carly Miller On Behalf of: Sheila Suurmeier, Black Hills Corporation, 5, 6, 1, 3; - Carly Miller	
Answer	
Document Name	
Comment	
Black Hills Corporation agrees with PNMR and has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.	
Likes 0	
Dislikes 0	

Response	
See PNMR response. The SDT is not authorized in the SAR to revise all of the standards. By having the low impact contained in CIP-002 and CIP-003, this allows “low impact only Entities” to comply with those two standards.	
Josh Combs - Black Hills Corporation – 3	
Answer	
Document Name	
Comment	
Black Hills Corporation agrees with PNMR and has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.	
Likes 0	
Dislikes 0	
Response	
See PNMR response. The SDT is not authorized in the SAR to revise all of the standards. By having the low impact contained in CIP-002 and CIP-003, this allows “low impact only Entities” to comply with those two standards.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
WECC suggests that the DT consider aligning the wording in Attachment 1 Sections 3.1.5 and 3.1.6 to match the working identified in Attachment 2 Section 3 items #5 and #6, specifically Section 3.1.6.	
Likes 0	
Dislikes 0	

Response	
Change made. The SDT has reviewed your comments and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
The NAGF has no additional comments.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority – 5	
Answer	
Document Name	
Comment	
None at this time.	
Likes 0	
Dislikes 0	
Response	

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. – 1	
Answer	
Document Name	
Comment	
Thank you for the ability to comment.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico – 1	
Answer	

Document Name	
Comment	
While PNMR does agree that coordinated attacks present risk, it is unclear as to the realized risk associated with a coordinated attack utilizing multiple low-impact BES Cyber Systems. As it would be difficult to quantify the number of low-impact systems needed to be utilized in a potential coordinated attack and with uncertain findings as to the use of low-impact systems to conduct a coordinated attack, PNM believes the potential risk to the BES from such attacks does not sufficiently correlate with the proposed authentication and detection controls which would be a vast expansion of scope. The NERC Low Impact Criteria Review Report references the risk of coordinated attacks on low impact BES Cyber Systems for those systems that are determined by the CIP-002 Standards. However, the CIP-002 categorization of BES Cyber Systems is not intended to take into account the effect of a coordinated attack in determining the categorization of a BES Cyber System. This language seems to attempt to change the purpose and muddy the scope of the CIP-002 Standard. PNMR also has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.	
Likes 0	
Dislikes 0	
Response	
The LICRT indicated they do not recommend changing the CIP-002 impact rating criteria used in identifying and categorizing individual BES Cyber Systems. Changes to CIP-002 are not included in the scope of the SAR for this project. The SDT is not authorized in the SAR to revise all of the standards. By having the low impact contained in CIP-002 and CIP-003, this allows “low impact only Entities” to comply with those two standards.	
Andrew Smith - APS - Arizona Public Service Co. – 5	
Answer	
Document Name	
Comment	

AZPS has no additional comments as this time.	
Likes 0	
Dislikes 0	
Response	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
For this statement, there may be a discrepancy in count: "Lower VSL *The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the seven topics required by R1. (R1.2)"* Should this be six instead of seven?	
Likes 0	
Dislikes 0	
Response	
Change made to all VSLs. Thank you for your comment.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	

Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 – RF	
Answer	
Document Name	
Comment	
Lower VSL *The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the seven topics required by R1. (R1.2)* Should this be six topics required by R1?	
Likes 0	
Dislikes 0	
Response	
Change made to all VSLs. Thank you for your comment.	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
(None)	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	

Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	
Document Name	
Comment	
In general, it seems that the SDT has expanded the requirements beyond what was recommended by the LICRT. For example, the LICRT stated there should be a requirement for the "detection of malicious communications to/between assets containing low-impact BES Cyber Systems with ERC." This languages allows greater flexibility in determining the location of detection compared to the SDT's specification of "for both inbound and outbound electronic remote access." Given that access is defined by communication "outside the asset containing low-impact BES Cyber System(s)," this language inherently mandates the detection to occur at he border of the low-impact asset.	
Likes 0	
Dislikes 0	
Response	
The verbiage "both inbound and outbound" and "outside the asset containing low-impact BES Cyber System(s)" is included in the currently approved CIP-003-9 Standard. The SDT has reused this verbiage to consistently address all remote access (in addition to vendor	

remote access addressed in CIP-003-9) to satisfy the revisions necessary to address the SAR. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification. The SDT removed the term "remote" from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	
Document Name	
Comment	
In general, it seems that the SDT has expanded the requirements beyond what was recommended by the LICRT. For example, the LICRT stated there should be a requirement for the "detection of malicious communications to/between assets containing low-impact BES Cyber Systems with ERC." This languages allows greater flexibility in determining the location of detection compared to the SDT's specification of "for both inbound and outbound electronic remote access." Given that access is defined by communication "outside the asset containing low-impact BES Cyber System(s)," this language inherently mandates the detection to occur at he border of the low-impact asset	
Likes 0	
Dislikes 0	
Response	
The verbiage "both inbound and outbound" and "outside the asset containing low-impact BES Cyber System(s)" is included in the currently approved CIP-003-9 Standard. The SDT has reused this verbiage to consistently address all remote access (in addition to vendor remote access addressed in CIP-003-9) to satisfy the revisions necessary to address the SAR. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to	

improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification. The SDT removed the term “remote” from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	
Document Name	
Comment	
We would like to thank the SDT for their hard work.	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	
Document Name	
Comment	
Constellation has no additional comments. Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	