NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2023-04 Modifications to CIP-003 | Draft 2
Comment Period Start Date:	1/30/2024
Comment Period End Date:	3/14/2024
Associated Ballot(s):	2023-04 Modifications to CIP-003 CIP-003-A AB 2 ST 2023-04 Modifications to CIP-003 Implementation Plan AB 2 OT

There were 71 sets of responses, including comments from approximately 169 different people from approximately 111 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 explain why and 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 explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

3. The Drafting Team (DT) 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 DT 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 DT 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
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
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
					Husam Al-Hadidi	Manitoba Hydro (System Performance)	1,3,5,6	MRO

Kimberly Bentley	Western Area Power Administration	1,6	MRO
Jaimin Patal	Saskatchewan Power Corporation (SPC)	1	MRO
George Brown	Pattern Operators LP	5	MRO
Larry Heckert	Alliant Energy (ALTE)	4	MRO
Terry Harbour	MidAmerican Energy Company (MEC)	1,3	MRO
Dane Rogers	Oklahoma Gas and Electric (OG&E)	1,3,5,6	MRO
Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
Michael Ayotte	ITC Holdings	1	MRO
Andrew Coffelt	Board of Public Utilities-Kansas (BPU)	1,3,5,6	MRO
Peter Brown	Invenergy	5,6	MRO

					Angela Wheat	Southwestern Power Administration	1	MRO
					Bobbi Welch	Midcontinent ISO, Inc.	2	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
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
Southern Company - Southern Company Services, Inc.	Jennifer Tidwell	1,3,5,6	SERC	Southern Company	Leslie Burke	Southern Company - Southern Company Generation	5	SERC
					Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Ron Carlsen	Southern Company - Southern	6	SERC

						Company Generation		
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
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
					Nick Fogleman	Prairie Power, Inc.	1,3	SERC
					Cooper Cash	North Carolina Electric Membership Corporation	3,4,5	SERC
Public Utility District No. 2 of Grant County, Washington	Karla Weaver	4		GCPD Group	Karla Weaver	Grant County PUD	4	WECC
					Nikkee Hebdon	Public Utility District No. 2 of Grant County, Washington	5	WECC
					Joanne Anderson	Public Utility District No. 2 of Grant	1	WECC

						County, Washington		
					Mike Stussy	Public Utility District No. 2 of Grant County, Washington	6	WECC
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
Black Hills Corporation	Rachel Schuldt	6		Black Hills Corporation - All Segments	Micah Runner	Black Hills Corporation	1	WECC
					Josh Combs	Black Hills Corporation	3	WECC
					Rachel Schuldt	Black Hills Corporation	6	WECC

					Carly Miller	Black Hills Corporation	5	WECC
					Sheila Suurmeier	Black Hills Corporation	5	WECC
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 Edison Co. of New York	1	NPCC
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 Resources, Inc.	5	NA - Not Applicable
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
Santee Cooper	Vicky Budreau	3		Santee Cooper	Rene' Free	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC

1. Do you agree with the language proposed in CIP-003-A Attachment 1? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.	
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 does not agree with the wording of Attachment 1, Section 3.1.3 which states:

"Authenticate users when permitting **each user-initiated instance** of electronic access to a network(s) containing low impact BES Cyber Systems;"

It is not feasible to authenticate each user-initiated instance of electronic access since doing so limits the technical solutions for implementing such a control. For example – if a registered entity were to implement a jump host solution, a user may be able to authenticate to the jump host and be permitted to access the low impact BES Cyber System based on successfully authenticating to the jump host. If the user established multiple connections from the jump host into multiple low impact BES Cyber Systems at different low impact assets, the proposed language may be interpreted as requiring additional authentication for each connection to other low impact BES Cyber Systems.

Section 3.1.3 as currently written is stricter than the high or medium impact Interactive Remote Access (IRA) requirements where “each user-initiated instance” of IRA ***DOES NOT*** require additional authentication for each connection. SMUD recommends the Standards Drafting Team change the language in Section 3.1.3 to read: “3.1.3 Authenticate users prior to permitting user-initiated electronic access to a network(s) containing low impact BES Cyber Systems;” This suggested wording aligns better with the SAR, whereas the existing wording does not indicate that users must be authenticated ***before*** access is granted to networks containing low impact BES Cyber Systems. The way in which Section 3.1.3 is currently written, it is as if the connection requires the authentication rather than the user being authenticated. SMUD also recommends the Standards Drafting Team make the following conforming changes to the language in Section 3.1.4 to read: “3.1.4 Protect user authentication information for user-initiated electronic access while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and • the authentication system used to meet Section 3.1.3, or • the asset containing low impact BES Cyber System(s);”	
Likes 2	Orlando Utilities Commission, 5, Colon Dania; American Municipal Power, 5, Ritts Amy
Dislikes 0	
Response	
Thank you for your comments. The drafting team (DT) made changes in Part 3.1.3 to address these comments. For Part 3.1.4, conforming changes were made to support the changes made in Part 3.1.3.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	

NRG disagrees with the removal of the term "remote" when referencing "electronic remote access" throughout Attachment 1. Not only does this significantly expand the scope of the requirements with respect to any type of non-remote electronic access, but it also moves away from the original intent of the three recommendations initially proposed by the LICRT. NRG recommends expanding the definition of the current term "interactive remote access" to include Low Impact BES Cyber Systems and using that newly defined terminology throughout this requirement.	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Thank you for your comment. The DT made changes to clarify what is meant by "remote" without including that language. Please see the changes before Section 3.1.1. An explanation on the purpose for removing "remote" has also been add to the TR.	
James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	
Section 3.2 states the Responsible Entity shall implement a control(s) that authenticates all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability. Section 3.2 should be removed, and Dial-up connectivity should be excluded from CIP-003-A regulations for LOW impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT made no material modifications to Section 3.2, this part of the standard has been in effective since it was passed with the Version 5 project.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
NRG disagrees with the removal of the term “remote” when referencing “electronic remote access” throughout Attachment 1. Not only does this significantly expand the scope of the requirements with respect to any type of non-remote electronic access, but it also moves away from the original intent of the three recommendations initially proposed by the LICRT. NRG recommends expanding the definition of the current term “interactive remote access” to include Low Impact BES Cyber Systems and using that newly defined terminology throughout this requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT made changes to clarify what is meant by “remote” without including that language. Please see the changes before Section 3.1.1. An explanation on the purpose for removing “remote” has also been add to the TR.	
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	
It appears that the Attachment 1 Section 3, Part 3.1.3 language is not restricted to the initial user authentication to a central management system that controls the access to multiple low impact BCS, as was intended by the SDT. Additionally, the lead-in statement in Section 3.1	

(and i-iii) defines what type of access to control, and it appears that the access described in the current Section 3.1.3 would not be in-scope of the electronic access defined in Section 3.1, and therefore would not create a required control. This is due to Section 3.1 (i) defining access as "between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing…", not "between a network containing a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing…".

Tacoma Power suggests the following language for Section 3.1.3:

"Authenticate user-initiated electronic access to a network(s) containing low impact BES Cyber Systems prior to establishing access applicable to Section 3.1;"

Note this change may be better as a new section in Attachment 1, for example, Section 3.3.

The above change would also lead to conforming changes in Section 3.1.4, as follows:

"Protect user authentication information for user-initiated electronic access while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and:

• the authentication system used to meet Section 3.1.3, or

• the asset containing low impact BES Cyber System(s);"

Likes 1	American Municipal Power, 5, Ritts Amy
Dislikes 0	

Response

Thank you for your comments. The drafting team (DT) made changes in Part 3.1.3 to address these comments. For Part 3.1.4, conforming changes were made to support the changes made in Part 3.1.3.

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

The wording in 3.1.3 as written could be read as requiring authentication each time a user accesses a network containing a Low Impact BES Cyber System, which would be stricter than the allowed jump host for medium and high impact requirements. Possible suggested wording to 3.1.3 are as follows:

"Authenticate users prior to user-initiated electronic access to a network(s) containing low impact BES Cyber Systems."

Or

"Authenticate users prior to user-initiated electronic access to a network(s) containing low impact BES Cyber Systems (multiple re-authentications are not required when accessing multiple sub networks within a larger network)"

The wording for 3.1.4 should be updated as well to match the suggested wording in 3.1.3:

"Protect authenticated information for user-initiated electronic access while in transit between …."

Likes 0	
Dislikes 0	

Response

Thank you for your comments, the DT made clarifying changes to 3.1.3 to address this comment that multiple re-authentications are not required.

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

Answer	No
Document Name	

Comment

Section 3.2 states the Responsible Entity shall implement a control(s) that authenticates all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 3.2 should be removed, and Dial-up connectivity should be excluded from CIP-003-A regulations for LOW impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, the DT made no material modifications to Section 3.2, this part of the standard has been in effective since it was passed with the Version 5 project.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Although section 3.1.2 is within the scope of the SAR, BPA still believes it creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers and inconsistencies within the standards. 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 or the applicability be changed to bring it in-line with other requirements.	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Thank you for your comments, the DT has responded to the requirements of the SAR which was based on the results of the Low Impact Criteria Review Team paper.	

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Matthew Jaramilla, 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	
Salt River Project agrees and supports comments from SMUD and Tacoma Power.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see the response to SMUD.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
Requirement 3.1.4 is not clear regarding what protection of the user authentication information is required. Please work to consolidate 3.1.3 and 3.1.4. The objectives are unclear. While substantial clarity was provided in the explanatory Webex, the proposed language lacks that clarity.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, The DT made clarifying changes to 3.1.3 and 3.1.4 to address comments. What needs to be protected will depend on architecture and technology implemented by each Responsible Entity. The DT does not intend to prescribe what needs to be	

protected in the standard. The Technical Rationale for part 3.1.4 included some examples of what should be protected "…protect the user authentication information (e.g. username, password, MFA information, session token, etc)"	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	

SMUD does not agree with the wording of Attachment 1, Section 3.1.3 which states:

"Authenticate users when permitting **each user-initiated instance** of electronic access to a network(s) containing low impact BES Cyber Systems;"

It is not feasible to authenticate each user-initiated instance of electronic access since doing so limits the technical solutions for implementing such a control. For example – if a registered entity were to implement a jump host solution, a user may be able to authenticate to the jump host and be permitted to access the low impact BES Cyber System based on successfully authenticating to the jump host. If the user established multiple connections from the jump host into multiple low impact BES Cyber Systems at different low impact assets, the proposed language may be interpreted as requiring additional authentication for each connection to other low impact BES Cyber Systems.

Section 3.1.3 as currently written is stricter than the high or medium impact Interactive Remote Access (IRA) requirements where "each user-initiated instance" of IRA ***DOES NOT*** require additional authentication for each connection.

SMUD recommends the Standards Drafting Team change the language in Section 3.1.3 to read:

"3.1.3 Authenticate users prior to permitting user-initiated electronic access to a network(s) containing low impact BES Cyber Systems;"

This suggested wording aligns better with the SAR, whereas the existing wording does not indicate that users must be authenticated ***before*** access is granted to networks containing low impact BES Cyber Systems. The way in which Section 3.1.3 is currently written, it is as if the connection requires the authentication rather than the user being authenticated.

SMUD also recommends the Standards Drafting Team make the following conforming changes to the language in Section 3.1.4 to read:

"3.1.4 Protect user authentication information for user-initiated electronic access while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and • the authentication system used to meet Section 3.1.3, or • the asset containing low impact BES Cyber System(s);"	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT made clarifying changes for Attachment 1, Part 3.1.3 to address these changes. For Part 3.1.4, conforming changes were made to support the changes made in Part 3.1.3. Please see the Technical Rationale for more information.	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
Southern Indiana Gas and Electric (SIGE) appreciate the work of the drafting team to address previous feedback provided for CIP-003-A Attachment 1. SIGE suggests the following changes in bold in order to qualify the type of access that is being addressed by this standard. The use of the verbiage "user-initiated instance of electronic access" could easily be interpreted as any user log-in. The act of a user logging into a local HMI at a substation is technically a "user-initiated instance of electronic access ." The suggested changes are intended to mimic the Interactive Remote Access term as defined in the NERC Glossary of terms, while not making any reference to an ESP. 3.1.3 Authenticate users when permitting each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, to a network(s) containing low impact BES Cyber Systems; 3.1.4 Protect user authentication information for each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and	

• the authentication system used to meet Section 3.1.3, or • the asset containing low impact BES Cyber System(s); 3.1.5 Include one or more method(s) for determining vendor electronic **remote** access, **not including system-to-system process communications**, where vendor electronic **remote** access, **not including system-to-system process communications**, is permitted; and 3.1.6 Include one or more method(s) for disabling vendor electronic **remote** access, **not including system-to-system process communications**, where vendor electronic **remote** access, **not including system-to-system process communications**, is permitted.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The drafting team (DT) made changes in Part 3.1.3 to address these comments. For Part 3.1.4, conforming changes were made to support the changes made in Part 3.1.3. These changes were made to clarify that 3.1.3 and 3.1.4 only apply to user based electronic access. The DT has chosen not to implement these changes as 3.1.5 and 3.1.6 are intended to capture both user based and system to system electronic access. This terminology was taken from the currently approved version of CIP-003-9 Attachment 1 section 6, and as there have been no material changes made to this requirement language, this DT is interested in preserving the associated language.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State agrees with SMUD's comments below: SMUD does not agree with the wording of Attachment 1, Section 3.1.3 which states:	

"Authenticate users when permitting **each user-initiated instance** of electronic access to a network(s) containing low impact BES Cyber Systems;" It is not feasible to authenticate each user-initiated instance of electronic access since doing so limits the technical solutions for implementing such a control. For example – if a registered entity were to implement a jump host solution, a user may be able to authenticate to the jump host and be permitted to access the low impact BES Cyber System based on successfully authenticating to the jump host. If the user established multiple connections from the jump host into multiple low impact BES Cyber Systems at different low impact assets, the proposed language may be interpreted as requiring additional authentication for each connection to other low impact BES Cyber Systems. Section 3.1.3 as currently written is stricter than the high or medium impact Interactive Remote Access (IRA) requirements where "each user-initiated instance" of IRA ***DOES NOT*** require additional authentication for each connection. SMUD recommends the Standards Drafting Team change the language in Section 3.1.3 to read: "3.1.3 Authenticate users prior to permitting user-initiated electronic access to a network(s) containing low impact BES Cyber Systems;" This suggested wording aligns better with the SAR, whereas the existing wording does not indicate that users must be authenticated ***before*** access is granted to networks containing low impact BES Cyber Systems. The way in which Section 3.1.3 is currently written, it is as if the connection requires the authentication rather than the user being authenticated. SMUD also recommends the Standards Drafting Team make the following conforming changes to the language in Section 3.1.4 to read: "3.1.4 Protect user authentication information for user-initiated electronic access while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and • the authentication system used to meet Section 3.1.3, or • the asset containing low impact BES Cyber System(s);"

Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The SDT made clarifying changes for Attachment 1, Part 3.1.3 to address these changes. For Part 3.1.4, conforming changes were made to support the changes made in Part 3.1.3. Please see the Technical Rationale for more information.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends aligning language with CIP-005-7 language or first focusing on modifying CIP-005-7 language prior to adjusting language for CIP-003-A.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has attempted to clarify the language to model CIP-005 as much as possible, however many NERC defined terms and other requirements in CIP-005 are not applicable to CIP-003 and Low Impact Systems, thus complete alignment is not possible.	
Carver Powers - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
The verbiage scoping required controls to the identified communication paths is eliminated in the proposed drafted language. Recommend clearly scoping the controls from 3.1.1 through 3.1.6 to the communications identified in 3.1 i-iii. Without this clarification: 1. There is no determination of the boundary for inbound and outbound in 3.1.1 and 3.1.2 2. 3.1.3 would require authentication for all user logins, including local logins.	

3. 3.1.5 and 3.1.6 would apply to vendors using TCAs. The information in Attachment 2 states "electronic access meets the criteria specified in Section 3.1" for 3.1.1 through 3.1.6, this language should be included in Attachment 1. The phrase “User initiated instance electronic access” should align more closely with the first sentence of the Interactive Remote Access definition to provide consistency and clarity. Without this clarity the language could include system to system communications. Recommending using a more consolidated term than “inbound and outbound electronic access”. If meaning bi-directional, then the standard should state that versus drawing a distinction between inbound and outbound.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT made some clarifying changes to the end of Section 3.1 to explicitly state its subparts 3.1.1 - 3.1.6 are only scoped for electronic access that meets the three romanettes embedded in Section 3.1. Since these subparts only apply to electronic access as described in romanette (i), the examples provided in your comment about local logins and TCA usage would not be in scope, so long as these connections are not traversing the asset boundary. The DT made changes to subparts 3.1.3 and 3.1.4 to clarify these subparts only apply to user-based electronic access. After a thorough review, the DT has decided that consolidating “inbound and outbound electronic access” to the term "bi-directional" could produce additional confusion due to instances that may arise where inbound and outbound electric access is not bi-directional. Therefore the DT has decided not to make any changes.	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

Santee Cooper does not agree with the wording of Attachment 1, Section 3.1.3 which states: "Authenticate users when permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems;"

It would be difficult to authenticate each user-initiated instance of electronic access. For example, if a user established multiple connections from the jump host into multiple low impact assets, the proposed language may be interpreted as requiring additional authentication for each connection to other low impact assets. This would make the CIP-003 Attachment 1, Section 3.1.3 requirement stricter than the high or medium impact Interactive Remote Access (IRA) requirement that doesn't require additional authentication for each connection.

In addition, the existing wording does not indicate that users must be authenticated before access is granted to a network(s) containing low impact assets. The way 3.1.3 is currently written, it is as if the connection requires the authentication rather than the user being authenticated.

Likes 0	
Dislikes 0	

Response

Thank you for your comments, the DT made clarifying changes to 3.1.3 to address this comment that multiple re-authentications are not required.

Alain Mukama - Hydro One Networks, Inc. - 1

Answer	No
Document Name	

Comment

For both sub-requirements 3.1.5 and 3.1.6 in Attachment 1, clarification is required on whether it includes both Interactive Remote Access and system-to-system remote access.

Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The DT didn't make material changes to 3.1.5 and 3.1.6. The previous DT stated that both interactive access and system to system was included.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
MRO interprets the draft Requirement language in Section 3.1.3 such that authentication is required each time a user initiates electronic access to any network(s) containing low impact BCSs. This interpretation of the language does not support the single authentication asserted by the SDT during the Project 2023-04 Webinar, relating to the jumphost in Figure 5 in the Technical Rationale. MRO recommends the Requirement language in Section 3.1.3 be changed to support the SDT's assertions. Any changes to the Requirement language needs to ensure that any electronic access directly from a network containing low impact BES Cyber Asset to a different network(s) containing low impact BES Cyber Systems, when not using a centralized electronic access system (e.g. jumphost), still requires authentication. Recommended language change: **Authenticate users prior to permitting user-initiated instances of electronic access to a network(s) containing low impact BES Cyber Systems**	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT made clarifying changes to 3.1.3 to address this comment that multiple re-authentications are not required.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	No
Document Name	

Comment
Attachment 1 appears to have exceeded the CIP-003 R2 (documented cybersecurity plan) due to the amount of technical controls that have now been added. Recommendation: if the SDT intends to keep expanding controls beyond the documented plans they should consider creating a new requirement. Why is this phrase used “User initiated instance electronic access”. Recommending using a more consolidated term than “inbound and outbound electronic access”. If meaning bi-directional, then the standard should state that versus drawing a distinction between inbound and outbound. Sub requirement 3.15, request clarification on whether the sub requirement applies to both system to system and user-initiated access by a vendor.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The purpose of Attachment 1 is to define any technical requirements for Low Impact BES. Hence DT team updated the attachment for consistency. The need for a new requirement can be discussed with NERC but that is not in-scope for this team. The DT 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. Additionally, the DT asserts that this is beyond the scope of the SAR. After a thorough review, the DT has decided that consolidating “inbound and outbound electronic access” to the term "bi-directional" could produce additional confusion due to instances that may arise where inbound and outbound electric access is not bi-directional. Therefore the DT has decided not to make any changes.

The DT didn't make material changes to 3.1.5 and 3.1.6. The previous DT stated that both interactive access and system to system was included.
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

Answer	No
Document Name	

Comment
NCPA supports comments made by SMUD and Tacoma Power.

Likes 0	
Dislikes 0	

Response
Thank you for your comments, please see response to SMUD.
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment
EEI appreciates the work of the drafting team to address previous feedback provided for CIP-003-A Attachment 1, but proposes the following modifications to Section 3, Part 3.1.3: "Authenticate users **prior to** permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems **(multiple re-authentications to sub-networks within a larger network are not required)**;"

We also suggest including clear language in the implementation guidance describing the change from use of the term remote access to electronic access including the relationship between the term electronic access and scoping language used in Section 3, Part 3.1, i-iii.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, the DT made clarifying changes to 3.1.3 to address this comment that multiple re-authentications are not required.	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	No
Document Name	
Comment	
The term “user-initiated instance” needs to be further clarified. We require more clarification on how much weight the technical rationale will have in interpreting compliance with Sections 3.1.3 and 3.1.4 with regulators when completing compliance monitoring activities. We believe the removal of the word “remote” from Section 3.1.3 in permitting user-initiated instances can create confusion on when a user is required to authenticate.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT clarified requirements within the Technical Rationale, and made clarifying changes to the standards with removal of “user-initiated instance”. The DT cannot speak on behalf of compliance related activities. Remote is defined in romanette (i).	
Richard Vendetti - NextEra Energy - 5	
Answer	No

Document Name	
Comment	
NEE's initial interpretation of CIP-003 Attachment 1 Section 3.1 was that the SDT's goal for inbound and outbound malicious communications protection was tied to firewalls or routers at each low BES Asset. However, the current language does not provide flexibility for managing inbound and outbound malicious communication security controls centrally, as illustrated in the Technical Rationale for Section 3.1.2. The standard language appears to imply medium impact Electronic Security Perimeter (ESP) and Electronic Access Point (EAP) protections at each low impact BES Asset without explicitly stating this. Section 3.1.4's authentication communication protection implies encryption at each remote cyber asset, exceeding medium impact requirements with Intermediate Systems. The Low Impact Criteria Review Team's (LICRT) intent was to address risk reduction for coordinated attacks on low BES Assets. Management of low impact security controls for authentication and malware mitigation, either locally or centrally, should be accommodated in Section 3.1 language. Implying controls are mandated at each low BES Asset goes beyond the LICRT's effort. While the Technical Rationale illustration for Section 3.1.2 provides for central aggregation, it does not address Section 3.1.4 if encrypted authentication communications pass through a central malware mitigation system for inbound and outbound traffic. The SDT should consider adjusting the language to allow both centralized and local security control options and clarify what options are available.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, the DT has made clarifying changes in both the Technical Rationale and the standard.	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
The language used should prioritize risk-based assessment with a focus on operational impact.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, the DT has made clarifying changes in both the Technical Rationale and the standard.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy Houston Electric (CEHE) appreciates the work of the drafting team to address previous feedback provided for CIP-003-A Attachment 1. CEHE suggests the following changes in bold in order to qualify the type of access that is being addressed by this standard. The use of the verbiage "user-initiated instance of electronic access" could easily be interpreted as any user log-in. The act of a user logging into a local HMI at a substation is technically a "user-initiated instance of electronic access ." The suggested changes are intended to mimic the Interactive Remote Access term as defined in the NERC Glossary of terms, while not making any reference to an ESP. 3.1.3 Authenticate users when permitting each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, to a network(s) containing low impact BES Cyber Systems;	

3.1.4 Protect user authentication information for each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and • the authentication system used to meet Section 3.1.3, or • the asset containing low impact BES Cyber System(s); 3.1.5 Include one or more method(s) for determining vendor electronic **remote** access, **not including system-to-system process communications**, where vendor electronic **remote** access, **not including system-to-system process communications**, is permitted; and 3.1.6 Include one or more method(s) for disabling vendor electronic **remote** access, **not including system-to-system process communications**, where vendor electronic **remote** access, **not including system-to-system process communications**, is permitted. Do you agree with the language proposed in CIP-003-A Attachment 2? If you do not agree, please explain why, and provide recommended language you would support and, if appropriate, technical, or procedural justification.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The drafting team (DT) made changes in Part 3.1.3 to address these comments. For Part 3.1.4, conforming changes were made to support the changes made in Part 3.1.3. These changes were made to clarify that 3.1.3 and 3.1.4 only apply to user based electronic access. The DT has chosen not to implement these changes as 3.1.5 and 3.1.6 are intended to capture both user based and system to system electronic access. This terminology was taken from the currently approved version of CIP-003-9 Attachment 1 section 6, and as there have been no material changes made to this requirement language, this DT is interested in preserving the associated language. The DT made changes to clarify what is meant by “remote” without including that language. Please see the changes before Section 3.1.1. An explanation on the purpose for removing “remote” has also been add to the TR.

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

Comment	
Dominion Energy supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
It is NST's understanding, based on the Technical Rationale document and the SDT's March 6, 2024 project webinar, that once a remote user has been authenticated in accordance with proposed requirement 3.1.3 and allowed to access a network containing low impact BCS, a Responsible Entity could, if it was so inclined, allow that user to connect to multiple BCS within that network, without re-authentication, for the duration of any given instance of remote electronic access. We believe that 3.1.3 should be modified to make this clear.	
Likes 1	LS Power Development, LLC, 5, Campbell C. A.
Dislikes 0	
Response	
Thank you for your comment. The DT made clarifying changes to 3.1.3 to address this comment that multiple re-authentications are not required.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	No
Document Name	

Comment	
LS Power Development agrees with comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
Seminole Electric votes negative because the standard drafting team has failed to justify within their technical rationale the need and the basis for all of the additional requirements for low impact sites	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see the background information in the Technical Rationale and the LICRT report for the rationale of the need.	
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	

Attachment 1 appears to have exceeded the CIP-003 R2 (documented cybersecurity plan) due to the amount of technical controls that have now been added.

Recommendation: if the SDT intends to keep expanding controls beyond the documented plans they should consider creating a new requirement.

Why is this phrase used “User initiated instance electronic access”. Recommending using a more consolidated term than “inbound and outbound electronic access”. If meaning bi-directional, then the standard should state that versus drawing a distinction between inbound and outbound.

Sub requirement 3.15, request clarification on whether the sub requirement applies to both system to system and user-initiated access by a vendor.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The purpose of Attachment 1 is to define any technical requirements for Low Impact BES. Hence DT team updated the attachment for consistency. The need for a new requirement can be discussed with NERC but that is not in-scope for this team.

The DT 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. Additionally, the DT asserts that this is beyond the scope of the SAR.

After a thorough review, the DT has decided that consolidating “inbound and outbound electronic access” to the term "bi-directional" could produce additional confusion due to instances that may arise where inbound and outbound electric access is not bi-directional. Therefore the DT has decided not to make any changes.

The DT didn't make material changes to 3.1.5 and 3.1.6. The previous DT stated that both interactive access and system to system was included.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, please see response to NPCC.	
Karla Weaver - Public Utility District No. 2 of Grant County, Washington - 4, Group Name GCPD Group	
Answer	No
Document Name	
Comment	
GCPD agrees and supports comments from SMUD and Tacoma Power about Appendix A section 3.13. This wording is more restrictive than IRAs utilized for Medium and High Impact access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to SMUD.	
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 challenge for 3.1.2 lies in the fact these terms used have acquired specific connotations, such as those associated with medium/high controls centers. Consequently, using these same words with different examples in the measures creates ambiguity in the expectations for compliance. The prescriptiveness of 3.1.3 and 3.1.4 seems to go beyond what is typically expected for Medium Impact.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, the DT has made conforming changes to the standard to match those approved in 2016-02. The DT notes that medium and high impact standards currently exist for remote access. The DT also notes that the required cyber security program for lows is not generally as strict or comprehensive as that for medium or high impact and also attempts to account for a wide diversity of entities that may have only low impact BCS. Medium and high 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 DT 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. Additionally, the DT asserts that this is beyond the scope of the SAR.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	

Comment	
Duke Energy supports the proposed langauge but also supports EEI's alternative language for added clarity.	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by MRO NSRF.	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Thank you for the comment, please see the response to MRO.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Time-sensitive communications of Protection Systems needs to be clearly defined.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments, the DT has made conforming changes to the standard to match those approved in 2016-02. Please see the standard revisions and CIP-005 Technical Rational drafted by the 2016-02 DT.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Thank you for considering and addressing the concerns by changing 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).	
Likes 0	
Dislikes 0	
Response	
The DT thanks you for your comment.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
For Section 3.1.3, the NSRF recommends changing "when" to "prior to" in order to clarify that the remote user be authenticated prior to access, as explained in the Technical Rationale.	

Additionally, the currently proposed language does not contain the clarification stated in the Technical Rationale that would allow a single authentication for user-initiated access to low impact BCS that reside in a sub-network contained within a larger network. The NSRF recommends adding a parenthetical to Section 3.1.3 to align with that intent. Example: 3.1.3 Authenticate users **prior to** permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems **(multiple re-authentications to sub-networks within a larger network are not required)**; MRO NSRF is of the belief that both of these suggested changes would be non-substantive and could be implemented prior to final ballot, if this ballot is successful.	
Likes 2	Orlando Utilities Commission, 5, Colon Dania; American Municipal Power, 5, Ritts Amy
Dislikes 0	
Response	
Thank you for the comment. The DT made changes in Part 3.1.3 to address these comments.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes

Document Name	
Comment	
For Section 3.1.3, Manitoba Hydro recommends changing “when” to “prior to” in order to clarify that the remote user be authenticated prior to access, as explained in the Technical Rationale. Additionally, the currently proposed language does not contain the clarification stated in the Technical Rationale that would allow a single authentication for user-initiated access to low impact BCS that reside in a sub-network contained within a larger network. Manitoba Hydro recommends adding a parenthetical to Section 3.1.3 to align with that intent. Example: 3.1.3 Authenticate users **prior to** when permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems **(multiple re-authentications to sub-networks within a larger network are not required)**; Manitoba Hydro is of the belief that both of these suggested changes would be non-substantive and could be implemented prior to final ballot, if this ballot is successful.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to MRO NSRF.	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	

Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with EEI's proposal for the following modifications to Section 3, Part 3.1.3: "Authenticate users **prior to** (*remove:* when) permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems **(multiple re-authentications to sub-networks within a larger network are not required);"** We also suggest including clear language in the implementation guidance describing the change from use of the term remote access to electronic access including the relationship between the term electronic access and scoping language used in Section 3, Part 3.1, i-iii.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	

Comment	
Southern Company is in agreement with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Jamie Monette - Jamie Monette On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Jamie Monette	
Answer	Yes
Document Name	
Comment	

The term user-initiated access creates ambiguity.	
Likes 0	
Dislikes 0	
Response	
The DT thanks you for your response, and has made clarifying changes to both the standard and the technical rationale.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF requests clarification regarding the language in section 3.1.3 for initial user-initiated access being adequate to move between low impact systems without additional authentication.	
Likes 0	
Dislikes 0	
Response	
The DT thanks you for your response. Clarifying changes have been made to show that one authentication should be sufficient.	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Recommended changes are in **bold**:	

3.1.3 Authenticate users **prior to** permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems **(multiple re-authentications to sub-networks within a larger network are not required)**;	
Likes 0	
Dislikes 0	
Response	
The DT thanks you for your response. Clarifying changes have been made to the standard. Please see the Technical Rationale for more information.	
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	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) and the MRO NSRF for questions #1.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the responses to EEI and MRO.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	

PNMR agrees with the language proposed in CIP-003-A Attachment 1. However, PNMR does agree with EEI in their suggestion to include clear language in the implementation guidance describing the change from the use of the term remote access to electronic access including the relationship between the term electronic access and scoping language used in Section 3, part 3.1, i-iii.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports EEI's comments.	

Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in alignment with the comments from the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is responding in alignment with the comments from the EEI.	
Likes 0	
Dislikes 0	
Response	

Thank you for the comment, please see response to EEI.	
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	
ACES approves of the proposed changes, but at some point, to make the standards clearer, we should consider distinguishing between "electronic access" a logical network connection and an individual's "electronic access" ie the ability to use credentials to log into a Cyber Asset.	
Likes 0	
Dislikes 0	
Response	
The DT thanks you for your response and support.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Selene Willis - Edison International - Southern California Edison Company - 5	

Answer	Yes
Document Name	
Comment	
See EEI Comments	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Kristina Marriott - Miller Bros. Solar, LLC - 5 - MRO,WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Thank you for your support.	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	

Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Patricia Ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

2. Do you agree with the language proposed in CIP-003-A Attachment 2? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.	
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	
Thank you for your comments, please see the DT's response to question 1.	
Karla Weaver - Public Utility District No. 2 of Grant County, Washington - 4, Group Name GCPD Group	
Answer	No
Document Name	
Comment	
Item 3 is the measure for section 3.1.3 which is too restrictive.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT created the examples listed in Attachment 2 not as an exhaustive list of how an entity must comply with the requirement, but rather to provide entities with examples of how they can demonstrate compliance with the requirements.	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	

Seminole Electric votes negative and does not agree because the standard drafting team has failed to justify within their technical rationale the need and the basis for all of the additional requirements for low impact sites	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT maintains the Technical Rationale provides background on the modifications made by the drafting team. The SAR and the LICRT report provide background on the justification for the changes.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	No
Document Name	
Comment	
LS Power Development agrees with comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments	

Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	

CEHE does not support the language proposed in CIP-003-A Attachment 2.

SIGE suggests the following changes in bold in order to qualify the type of access that is being addressed by this standard. The use of the verbiage “user-initiated instance of electronic access” could easily be interpreted as any user log-in. The act of a user logging into a local HMI at a substation is technically a “user-initiated instance of electronic access.” The suggested changes are intended to mimic the Interactive Remote Access term as defined in the NERC Glossary of terms, while not making any reference to an ESP.

Attachment 2, Section 3:

3. For Section 3.1.3, documentation showing the ability to authenticate users when permitting each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, where **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, to a network(s) containing low impact BES Cyber Systems, such as:

• Authentication mechanism(s) including but not limited to:

{C}§ Utilization of Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), and/or similar implemented solutions; or

{C}§ Enforcement of Multi-Factor Authentication (MFA).

• Virtual Private Network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;

• Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BES Cyber System; or

• Other operational, procedural, or technical controls.

4. For Section 3.1.4, documentation showing the ability to protect user authentication information for each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, where electronic **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and

• the authentication system used to meet Section 3.1.3, or

• the asset containing low impact BES Cyber System(s),

such as:

• Protection mechanism(s) including but not limited to:

{C}§ Implementation of an encrypted protocol or service (Hypertext Transfer Protocol Secure (HTTPS), Secure Shell (SSH), etc.); or

{C}§ Implementation of an IPsec or Secure Sockets Layer (SSL) VPN.

{C}§ Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic remote access, where vendor electronic **remote** access, **not including system-to-system process communication**s, is permitted and electronic **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, such as:

• Steps to preauthorize access;

• Alerts generated by vendor log on;

• Session monitoring;

• Security information management logging alerts;

• Time-of-need session initiation;

• Session recording;

• System logs; or

• Other operational, procedural, or technical controls.

6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic **remote** access, **not including system-to-system process communications**, where vendor electronic **remote** access, **not including system-to-system process communications**, is permitted and electronic **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, such as:

• Disabling vendor electronic **remote** access, **not including system-to-system process communications accounts**;

• Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic **remote** access, **not including system-to-system process communications**;

• Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic **remote** access, **not including system-to-system process communications**;

• Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);

• Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic **remote** access, **not including system-to-system process communications**; or

• Other operational, procedural, or technical controls.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The drafting team (DT) made changes in Part 3.1.3 to address these comments. For Part 3.1.4, conforming changes were made to support the changes made in Part 3.1.3. These changes were made to clarify that 3.1.3 and 3.1.4 only apply to user based electronic access. The DT has chosen not to implement these changes as 3.1.5 and 3.1.6 are intended to capture both user based and system to system electronic access. This terminology was taken from the currently approved version of CIP-003-9 Attachment 1 section 6, and as there have been no material changes made to this requirement language, this DT is interested in preserving the associated language. The drafting team made conforming changes to Attachment 2 due to the changes in Attachment 1.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
The language used should prioritize risk-based assessment with a focus on operational impact.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, the DT has made clarifying changes in both the Technical Rationale and the standard.	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	

Please updated Attachment 2 to include the updated Attachment 1 Section 3 controls requested in question 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has made conforming changes to Attachment 2 based on the updates made to Attachment 1.	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	No
Document Name	
Comment	
The additional discrete requirements and expansion to all inbound and outbound electronic access is a significant incremental increase in the requirements for low-impact assets. Pending on an organizations current cybersecurity maturity level, meeting and maintaining these requirements will take significant effort and cost. It is anticipated this will require entities to hire multiple additional full-time staff to maintain and partake in lengthy contract negotiations with OEMs and other remote access vendors to ensure the additional discrete details included in the language can be met. Although section 3.1.2 is within the scope of the SAR, we still believe it creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers and inconsistencies within the standards. 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). We suggest that this requirement be removed for better consistency with the requirements for Medium BCS or the applicability be changed to bring it in-line with other requirements.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT notes that medium and high impact standards currently exist for remote access. The DT also notes that the required cyber security program for lows is not generally as strict or comprehensive as that for medium or high impact and also attempts to account for a wide diversity of entities that may have only low impact BCS. Medium and high 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 DT 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. Additionally, the DT asserts that this is beyond the scope of the SAR.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI proposes the following revisions to align with the proposal provided in response to Question 1. "For Section 3.1.3, documentation showing the ability to authenticate users **prior to** permitting each user-initiated instance of electronic access, where electronic access meets the criteria specified in Section 3.1, to a network(s) containing low impact BES Cyber Systems, such as…"	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, the DT has made this change along with other conforming changes in response to updates made in Attachment 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	

Answer	No
Document Name	
Comment	
NCPA supports comments made by SMUD and Tacoma Power.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see SMUD and Tacoma Power responses.	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
In Attachment 2, Section 3, Example 2, in the list of examples the "Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)" is the only one of the bulleted list that meets the security objective of the SAR. For example: · "Anti malware technologies" are at the host level and are not a great option for detecting "malicious communications at the network level". The controls should be network based and not host based. · "Automated or manual log reviews" are too ambiguous, it would be best to specify what types of logs that would meet the security objective. Simply reviewing electronic access logs, for example, is not sufficient. · "Alerting" and "Other operational, procedural, or technical controls" should be removed since they provide no real guidance.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has included some new suggested examples under Attachment 2 (note: not an exhaustive list of every example).	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Attachment 1 - Ameren would like clarity in section 3.1.3. Is the Responsible Entity capable of relying on services/support vendors for user accounts and authentication? Attachment 2 - For section 3.1.5, Ameren would like clarity around the phrase "Security information management logging alerts." In CIP-007, this is described as "Security event monitoring."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. This DT believes the Project 2020-03 DT who worked on CIP-003-9 drew comparisons to the measure language offered in CIP-005-7 R2.4 when they were working on section 6. “Security information management logging alerts” is just one example out of many that can demonstrate compliance with section 3.1.5. This terminology was taken from the currently approved version of CIP-003-9 Attachment 2 section 6.1, and as there have been no material changes made to this requirement language, this DT is interested in preserving the associated guidance language.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	

Comment	
Reclamation recommends aligning language with CIP-005-7 language or first focusing on modifying CIP-005-7 language prior to adjusting language for CIP-003-A.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, the DT has responded to the requirements of the SAR which was based on the results of the Low Impact Criteria Review Team paper.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Please see response to question #1. Attachment 2 language would need to be updated based on the proposed changes in Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, please see the DT's response to question 1. The DT has made conforming changes to Attachment 2 based on the updates made to Attachment 1.	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	

SIGE suggests the following changes in bold in order to qualify the type of access that is being addressed by this standard. The use of the verbiage “user-initiated instance of electronic access” could easily be interpreted as any user log-in. The act of a user logging into a local HMI at a substation is technically a “user-initiated instance of electronic access.” The suggested changes are intended to mimic the Interactive Remote Access term as defined in the NERC Glossary of terms, while not making any reference to an ESP.

Attachment 2, Section 3:

3. For Section 3.1.3, documentation showing the ability to authenticate users when permitting each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, where **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, to a network(s) containing low impact BES Cyber Systems, such as:

• Authentication mechanism(s) including but not limited to:

{C}§ Utilization of Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), and/or similar implemented solutions; or

{C}§ Enforcement of Multi-Factor Authentication (MFA).

• Virtual Private Network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;

• Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BES Cyber System; or

• Other operational, procedural, or technical controls.

4. For Section 3.1.4, documentation showing the ability to protect user authentication information for each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, where electronic **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and

• the authentication system used to meet Section 3.1.3, or

• the asset containing low impact BES Cyber System(s),

such as:

• Protection mechanism(s) including but not limited to:

{C}§ Implementation of an encrypted protocol or service (Hypertext Transfer Protocol Secure (HTTPS), Secure Shell (SSH), etc.); or

{C}§ Implementation of an IPsec or Secure Sockets Layer (SSL) VPN.

{C}§ Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic remote access, where vendor electronic **remote** access, **not including system-to-system process communication**s, is permitted and electronic **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, such as:

• Steps to preauthorize access;

• Alerts generated by vendor log on;

• Session monitoring;

• Security information management logging alerts;

• Time-of-need session initiation;

• Session recording;

• System logs; or

• Other operational, procedural, or technical controls.

6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic **remote** access, **not including system-to-system process communications**, where vendor electronic **remote** access, **not including system-to-system process communications**, is permitted and electronic **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, such as: • Disabling vendor electronic **remote** access, **not including system-to-system process communications accounts**; • Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic **remote** access, **not including system-to-system process communications**; • Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic **remote** access, **not including system-to-system process communications**; • Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment); • Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic **remote** access, **not including system-to-system process communications**; or • Other operational, procedural, or technical controls.	
Likes 0	
Dislikes 0	
Response	
These changes were made to clarify that 3.1.3 and 3.1.4 only apply to user based electronic access. The DT has chosen not to implement these changes as 3.1.5 and 3.1.6 are intended to capture both user based and system to system electronic access. This terminology was taken from the currently approved version of CIP-003-9 Attachment 1 section 6, and as there have been no material changes made to this requirement language, this DT is interested in preserving the associated language. Conforming changes were made in Attachment 2 to align with the changes made in Attachment 1.	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No

Document Name	
Comment	

In Attachment 2, Section 3, Example 2, there is only one bullet in the list of examples provided that meet the security objective of the SAR. That example is “Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)”.

The other bullets are not good examples for the following reasons:

“Anti-malware technologies” are at the host level and is not a great control for detecting “malicious communications at the network level;” malicious code - YES, malicious communications - NO. The controls should be network based and not host based.

“Automated or manual log reviews” depending on how they are done, is not a great control. It would be best to specify what types of logs that would meet the security objective (e.g. Security Incident and Event Management logs, Netflow, Jflow etc.). Simply reviewing electronic access logs, for example, is not sufficient.

“Alerting” and “Other operational, procedural, or technical controls” do not add any value to the list of examples since they provide no real guidance.

SMUD recommends the Standards Drafting Team consider the following changes to Attachment 2, Section 3, Example 2:

“2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets the criteria specified in Section 3.1, such as:

• Anti-malware technologies; **[Delete]**

• Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)

- Monitor or alert for changes to communication baselines; [**Add]**
- Logging and alerting configuration for Security Incident and Event Management (SIEM) systems or other event correlation systems; [**Add]**

• Automated or manual log reviews; **[Delete]**

• Alerting; or **[Delete]** • Other operational, procedural, or technical controls**. [Delete]**	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has included some of the new suggested examples under Attachment 2 (note: not an exhaustive list).	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
Attachment 2, Section 3: All the Authentication Mechanisms identified represent some form of centralized account management. Due to economies of scale, reliability, this may not represent the best option. Additionally, it precludes usage of password vault tools that may provide effective security for managing credentials. Please re-word to allow flexibility of approach based on risk and technologies.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. While some of the examples in Attachment 2 include centralized authentication mechanisms, it is not the DT's intention to be an exhaustive/prescriptive list of only acceptable solutions. The DT understands that each Responsible Entity will have different architectures and thus included the last bullet "[or] Other operational, procedural, or technical controls" to allow each Responsible Entity flexibility in finding a tool that works for them.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Matthew Jaramilla, 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	
Salt River Project supports SMUD comments and also suggest deleting "automated or manual log reviews" and "alerting"	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to SMUD.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Although section 3.1.2 is within the scope of the SAR, BPA still believes it creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers and inconsistencies within the standards. 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 or the applicability be changed to bring it in-line with other requirements.	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	

Thank you for your comments. The DT notes that medium and high impact standards currently exist for remote access. The DT also notes that the required cyber security program for lows is not generally as strict or comprehensive as that for medium or high impact and also attempts to account for a wide diversity of entities that may have only low impact BCS. Medium and high 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 DT 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.	
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 updating the Attachment 2 language based on the proposed changes to Attachment 1, Section 3.1.3 (see response to Comment 1). Tacoma Power also endorses the comments provided by SMUD.	
Likes 1	American Municipal Power, 5, Ritts Amy
Dislikes 0	
Response	
Thank you for your comment, please see the DT's response to question 1. The DT has made conforming changes to Attachment 2 based on the updates made to Attachment 1. Additionally, see response to SMUD's comment.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No

Document Name	
Comment	
Please reference the comments in response to Question 1 above.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see the DT's response to question 1.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
NRG disagrees with the removal of the term "remote" when referencing "electronic remote access" throughout Attachment 1. Not only does this significantly expand the scope of the requirements with respect to any type of non-remote electronic access, but it also moves away from the original intent of the three recommendations initially proposed by the LICRT. NRG recommends expanding the definition of the current term "interactive remote access" to include Low Impact BES Cyber Systems and using that newly defined terminology throughout this requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT made changes to clarify what is meant by "remote" through romanette (i). Please see the changes before Section 3.1.1. An explanation on the purpose for removing "remote" has also been add to the Technical Rationale.	

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	

In Attachment 2, Section 3, Example 2, there is only one bullet in the list of examples provided that meet the security objective of the SAR. That example is “Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)”.

The other bullets are not good examples for the following reasons:

“Anti malware technologies” are at the host level and is not a great control for detecting “malicious communications at the network level;” malicious code - YES, malicious communications - NO. The controls should be network based and not host based.

“Automated or manual log reviews” depending on how they are done, is not a great control. It would be best to specify what types of logs that would meet the security objective (e.g. Security Incident and Event Management logs, Netflow, Jflow etc.). Simply reviewing electronic access logs, for example, is not sufficient.

“Alerting” and “Other operational, procedural, or technical controls” do not add any value to the list of examples since they provide no real guidance.

SMUD recommends the Standards Drafting Team consider the following changes to Attachment 2, Section 3, Example 2:

“2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets the criteria specified in Section 3.1, such as:

• Anti-malware technologies; [Delete]

• Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);

- Monitor or alert for changes to communication baselines; [Add]
- Logging and alerting configuration for Security Incident and Event Management (SIEM) systems or other event correlation systems; [Add]

• Automated or manual log reviews; [Delete]

• Alerting; or [Delete]

• Other operational, procedural, or technical controls. [Delete]

Likes 2	Orlando Utilities Commission, 5, Colon Dania; American Municipal Power, 5, Ritts Amy
Dislikes 0	

Response

Thank you for your comments. The DT has included some of the new suggested examples under Attachment 2 (note: not an exhaustive list).

Kristina Marriott - Miller Bros. Solar, LLC - 5 - MRO,WECC,Texas RE

Answer	No
Document Name	

Comment

Language throughout that states "such as" then listing multiple bullet points should be reworded to state: "one or more of the following". The “such as” verbiage may lead auditors to mark each item as being applicable.

Likes 0	
Dislikes 0	

Response

Thank you for your comment, the DT has decided to maintain the current language. The DT believes “such as” does afford flexibility to the Responsible Entity and does not prescribe a specific solution.

Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
See EEI Comments	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	

Comment	
Exelon is responding in alignment with the comments from the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in alignment with the comments from the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports EEI's comments.	

Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
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	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) and the MRO NSRF for questions #2.	
Likes 0	
Dislikes 0	

Response	
Thank you for the comment, please see the response to EEI.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF requests clarification for section 3.1.3 to understand if the Responsible Entity can rely on services/support vendors for their user accounts and authentication.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. You may refer to the CMEP Practice Guide on Using the Work of Others on how CMEP staff may treat this type of evidence.	
Jamie Monette - Jamie Monette On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Jamie Monette	
Answer	Yes
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Recommend modifying the language in Attachment 1 to align with the language in Attachment 2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has made conforming changes to Attachment 2 based on the updates made to Attachment 1.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company is in agreement with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes

Document Name	
Comment	
Black Hills Corporation agrees with EEI's proposal for the following revisions to align with the proposal provided in response to Question 1. "For Section 3.1.3, documentation showing the ability to authenticate users **prior to (*remove:* when)** permitting each user-initiated instance of electronic access, where electronic access meets the criteria specified in Section 3.1, to a network(s) containing low impact BES Cyber Systems, such as…"	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes

Document Name	
Comment	
Revise Section 3.1.3 based on Attachment 1 revisions recommended above.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see the DT's response to question 1.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	

The language in CIP-003A Attachment 2 is acceptable as long as the wording for 3.1.3 and 3.1.4 are modified/updated as suggested	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see the DT's response to question 1. The DT has made conforming changes to Attachment 2 based on the updates made to Attachment 1.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Revise Section 3.1.3 based on Attachment 1 revisions recommended above.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see the DT's response to question 1. The DT has made conforming changes to Attachment 2 based on the updates made to Attachment 1.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by MRO NSRF	

Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to MRO NSRF.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the proposed language but also supports EEI's alternative language for added clarity.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Patricia Ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
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	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
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	
Thank you for your support.	
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	
Thank you for your support.	
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	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

3. The Drafting Team (DT) 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.	
James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	
As Long as Dial-up is not in scope 3 years is agreeable. IF Dial-up is NOT removed, 3 years is not long enough.	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Thank you for your comment. Part 3.2 of Attachment 1 for authentication of dial-up were not materially changed as part of this project. The modifications that were made to Part 3.2 from CIP-003-9 were in formatting only. Changes or exclusion of requirement for dial-up are outside the scope of the approved SAR for this project.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	

AZPS agrees with EEI's proposal to align the implementation plans for CIP-003 changes resulting from Project 2016-02 and Project 2023-04 to avoid separate versions and implementation plans which will require entities to make changes affecting low impact BCS under different regulatory deadlines resulting in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
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	
Until Tacoma Power's concern on the language in Attachment 1 Section 3.1.3 is resolved to include only the initial authentication, this implementation plan is not achievable. However, if these concerns are addressed, then 36 months is reasonable timeframe.	
Likes 1	American Municipal Power, 5, Ritts Amy
Dislikes 0	
Response	
Thank you for your comment, please see responses to Questions 1 and 2.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No
Document Name	

Comment	
As Long as Dial-up is not in scope 3 years is agreeable. IF Dial-up is NOT removed, 3 years is not long enough.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Part 3.2 of Attachment 1 for authentication of dial-up were not materially changed as part of this project. The modifications that were made to Part 3.2 from CIP-003-9 were in formatting only. Changes or exclusion of requirement for dial-up are outside the scope of the approved SAR for this project.	
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 your comment, please see responses to questions 1 and 2.	
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 comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Matthew Jaramilla, 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	
Salt River Project agrees and supports comments from AZPS and EEI. In addition, SRP would like to have a specific date of implementation as there is significant cost associated with this project (equipment and resources), time for planning, and work that would need to be done.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see responses to AZPS and EEI. The implementation plan specifies a 3-year timeline after final approvals. Final approvals depend on successful balloting, NERC Board and FERC approvals which are unknown at this time.	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	

SIGE supports the comments as submitted by Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends that the CIP-003-A implementation plan consider the CIP-003-10 implementation plan to allow the effective use of resources.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. For this posting the drafting team included a CIP-003-12 draft standard and implementation plan which takes into account the timelines of the two versions of the standard.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company is in agreement with EEI comments.	

Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The NAGF recommends that the CIP-003-A implementation plan consider the CIP-003-10 implementation plan to allow the effective use of resources.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. For this posting the drafting team included a CIP-003-12 draft standard and implementation plan which takes into account the timelines of the two versions of the 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 (EEI) for question #3.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
NEE supports EEI's comments: "EEI proposes the alignment of the implementation plan for CIP-003 in Project 2016-02 with the 3-year implementation plan proposed in Project 2023-04 allowing entities to only make changes to the affected sites once. We further suggest combining the revisions to CIP-003 resulting from Project 2023-04 and 2016-02 into one version for NERC Board approval after passing ballot if they will be presented to the Board at the same meeting. Separate versions and implementation plans will require entities to make changes affecting low impact BCS	

under different regulatory deadlines resulting in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated."	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
The undertaking will demand significant effort, substantial capital investment and additional staffing.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. 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.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	

Comments: CEHE does not agree with the proposed implementation plan because of the pending changes in Project 2016-02. CEHE agrees with EEI's comment on the implementation plan. EEI Comments: EEI proposes the alignment of the implementation plan for CIP-003 in Project 2016-02 with the 3-year implementation plan proposed in Project 2023-04 allowing entities to only make changes to the affected sites once. We further suggest combining the revisions to CIP-003 resulting from Project 2023-04 and 2016-02 into one version for NERC Board approval after passing ballot if they will be presented to the Board at the same meeting. Separate versions and implementation plans will require entities to make changes affecting low impact BCS under different regulatory deadlines resulting in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
See comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	No
Document Name	
Comment	
As a parent company to a fleet of over 25 Low Impact Generation Facilities, along with affiliates with equally sizeable fleets, 36 months will not be enough time for owners with multiple Low Impact generation facilities to onboard these controls. Recommend a provision for owners with multiple Low Impact facilities allowing up to 5 years.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team has not made changes to the implementation plan and asserts that the drafted implementation timeline is in-line with similar standards changes.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	

Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
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	
Thank you for your comment. The revisions to CIP-003-9 were made based on the approved SAR and the DT appreciates that there may be cost associated with the implementation of the new standard.	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your 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	

SMUD agrees with a three-year implementation plan and believes it is the necessary amount of time for supply chains to support the changes registered entities will need to implement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the implementation plan, but also supports EEI's recommendation to align the implementation of the LICRT CIP-003 revisions with the implementation of the CIP-003 revisions from the 2016-02 Project.	
Likes 0	
Dislikes 1	Orlando Utilities Commission, 5, Colon Dania
Response	
Thank you for the comment, please see response to EEI.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by MRO NSRF	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to MRO NSRF.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
The 3 year implementation plan is sufficient unless there is a supply chain issue with the manufacturers of the equipment needed to implement this solution.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment.	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
OUC agrees with a three-year implementation plan and believes it is the necessary amount of time for supply chains to support the changes registered entities will need to implement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
If concerns are addressed in Attachment 1 then a 3 year implementation time is sufficient.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to other comments regarding Attachment 1.	

Jamie Monette - Jamie Monette On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Jamie Monette	
Answer	Yes
Document Name	
Comment	
Additional time should be considered to architect and implement authentication methods.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team has not made changes to the implementation plan and asserts that the drafted implementation timeline is in-line with similar standards changes.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI proposes the alignment of the implementation plan for CIP-003 in Project 2016-02 with the 3-year implementation plan proposed in Project 2023-04 allowing entities to only make changes to the affected sites once. We further suggest combining the revisions to CIP-003 resulting from Project 2023-04 and 2016-02 into one version for NERC Board approval after passing ballot if they will be presented to the Board at the same meeting. Separate versions and implementation plans will require entities to make changes affecting low impact BCS under different regulatory deadlines resulting in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated.	
Likes 1	Sempra - San Diego Gas and Electric, 5, Wright Jennifer
Dislikes 0	

Response	
Thank you for your comments. Thank you for your comment. For this posting the drafting team included a CIP-003-12 draft standard and implementation plan which takes into account the timelines of the two versions of the standard.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
See EEI Comments	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Mohamed Derbas - Sempra - San Diego Gas and Electric - 1	
Answer	Yes
Document Name	
Comment	
SDG&E supports EEI's comments on this item.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	

Kristina Marriott - Miller Bros. Solar, LLC - 5 - MRO,WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
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	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
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	

Thank you for your support.	
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	
Thank you for your support.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
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	
Thank you for your support.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
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	
Thank you for your support.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karla Weaver - Public Utility District No. 2 of Grant County, Washington - 4, Group Name GCPD Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Ireland - DTE Energy - 4	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
WECC leaves comments on the implementation plan to the applicable entities.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

4. The DT 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.	
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, using these same words with different examples in the measures creates ambiguity in the expectations for compliance.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT notes that medium and high impact standards currently exist for remote access. The DT also notes that the required cyber security program for lows is not generally as strict or comprehensive as that for medium or high impact and also attempts to account for a wide diversity of entities that may have only low impact BCS. Medium and high 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 DT 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. Additionally, the DT asserts that this is beyond the scope of the SAR.	
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	
Some entities implemented electronic access controls not expecting these added controls. The added malicious communication detection(s) may require a complete redesign to properly implement this control making it costly.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	No
Document Name	
Comment	

Since there is no cost recovery mechanism for generation facilities, from a business perspective, these technical controls and compliance processes have the potential to significantly impact the cost structure of support at each site. It would be accurate to say that we have the framework in place to support these technologies, but the concern would be the human-capital required to support the recurring maintenance of such processes. Because of how Low Impact Generation Facilities are setup, the objectives outlined in the proposed controls would require effort from IT/OT support providers, O&Ms, and OEMs. Needless to say, 36 months will not be enough time for owners with multiple Low Impact generation facilities to implement these requirements.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
The undertaking will demand significant effort, substantial capital investment and additional staffing.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems	

against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective.	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	No
Document Name	
Comment	
The additional discrete requirements and expansion to all inbound and outbound electronic access is a significant incremental increase in the requirements for low-impact assets. Pending on an organization's current cybersecurity maturity level, meeting and maintaining these requirements will take significant effort and cost. It is anticipated this will require entities to hire multiple additional full-time staff to maintain and partake in lengthy contract negotiations with OEMs and other remote access vendors to ensure the additional discrete details included in the language can be met.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective.	
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	
Answer	No
Document Name	
Comment	

NCPA supports comments made by SMUD and Tacoma Power.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, please see response to SMUD and Tacoma Power.	
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	
Thank you for your response, the DT has made clarifying changes to the standard.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends minimizing churn among standard versions and clearly identify the scope; Reclamation also recommends the DT take additional time to coordinate the modifications with other existing drafting teams for related standards. This will help minimize	

the costs associated with the planning and adjustments required to achieve compliance with frequently changing requirements. Reclamation will need more information to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The DT has worked with other teams to minimize the churn in the standards as much as possible. For this posting the drafting team included a CIP-003-12 draft standard and implementation plan which takes into account the timelines of the two versions of the standard.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State would need to have more details before costs could be accurately determined.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response, the DT has made clarifying changes to the standard.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	

NIPSCO has not determined whether this will be cost effective. The procurement process for a tool(s) and resources will be initiated should the requirement language remain as is.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective.	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
For small Entities implementation of the controls outlined in the proposed standard could be financially burdensome. Entities with a large number of Low stations may have difficulty meeting the 36 months implementation timeframe.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective.	

The drafting team has not made changes to the implementation plan and asserts that the drafted implementation timeline is in-line with similar standards changes.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
For small Entities implementation of the controls outlined in the proposed standard could be financially burdensome. Entities with a large number of Low stations may have difficulty meeting the 36 months implementation timeframe.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective. The drafting team has not made changes to the implementation plan and asserts that the drafted implementation timeline is in-line with similar standards changes.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Matthew Jaramilla, 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	

Salt River Project agrees and supports Tacoma's comment. In addition, SRP believes that more information required as it is difficult to determine the exact financial impact, even though we are expecting a significant cost that would need to be budgeted.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective. Additionally, the DT has made clarifying changes to the standard.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No
Document Name	
Comment	
As Long as Dial-up is not in scope the project can be performed in a cost-effective manner. IF Dial-up is not removed, the project will not be cost-effective.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Part 3.2 of Attachment 1 for authentication of dial-up were not materially changed as part of this project. The modifications that were made to Part 3.2 from CIP-003-9 were in formatting only. Changes or exclusion of requirement for dial-up are outside the scope of the approved SAR for this project.	

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	
It cannot be determined at this time if the SAR addresses the issues in a cost effective manner.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective. Additionally, the DT has made clarifying changes to the standard.	
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	
Until Tacoma Power's concern on the language in Attachment 1 Section 3.1.3 is resolved to include only the initial authentication, this is not a cost effective requirement, both in terms of upfront cost of implementing significant additional tooling, as well as ongoing stakeholder time to update and perform work practices in a compliant manner.	

Likes 1	American Municipal Power, 5, Ritts Amy
Dislikes 0	

Response

The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective.

Additionally, the DT has made clarifying changes to the standard.

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

Irrespective of cost effectiveness, NRG does not believe that the proposed changes address the original issues outlined in the SAR. Please reference comments in response to Question 1 above for additional detail.

Likes 0	
Dislikes 0	

Response

Thank you for your comments, please see response to question 1.

James Keele - Entergy - 3

Answer	No
Document Name	

Comment

As Long as Dial-up is not in scope the project can be performed in a cost-effective manner. IF Dial-up is not removed, the project will not be cost-effective.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Part 3.2 of Attachment 1 for authentication of dial-up were not materially changed as part of this project. The modifications that were made to Part 3.2 from CIP-003-9 were in formatting only. Changes or exclusion of requirement for dial-up are outside the scope of the approved SAR for this project.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
Irrespective of cost effectiveness, NRG does not believe that the proposed changes address the original issues outlined in the SAR. Please reference comments in response to Question 1 above for additional detail.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, please see response to question 1.	
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 views the changes as neither cost effective nor cost ineffective.	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Thank you for your response.	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your response.	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
See EEI Comments	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	

Answer	Yes
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	

No additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by MRO NSRF	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, please see response to MRO NSRF.	
Patricia Ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Karla Weaver - Public Utility District No. 2 of Grant County, Washington - 4, Group Name GCPD Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
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	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
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	
Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kristina Marriott - Miller Bros. Solar, LLC - 5 - MRO,WECC,Texas RE	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	
Document Name	
Comment	
ITC does not respond to cost questions	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	

NST lacks the information necessary to comment on this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, the DT has made clarifying changes in the standard.	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	
NEE does not comment on costs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Jamie Monette - Jamie Monette On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Jamie Monette	
Answer	
Document Name	
Comment	
NA	

Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren has no comment on the cost effectiveness of the project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	
Document Name	
Comment	
Black Hills Corporation will not comment on cost-effectiveness.	
Likes 0	
Dislikes 0	
Response	

Thank you for your response.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
WECC leaves comments on the cost-effectiveness to the applicable entities.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	

5. Provide any additional comments on the standard and technical rationale for the DT to consider, if desired.
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
Document Name
Comment
In the revised Technical Rationale document on page 7, the paragraph directly above Figure 4 references “Figure 4” but is actually referencing Figure 5. If confirmed and appropriate, the paragraph should be moved below Figure 4 and the text changed to say:

"***Figure 5*** depicts an example of protected authentication at a central intermediate system before accessing a network containing a LIBCS. This protection mitigates the unintended disclosure of authentication information for remote access of LIBCS."	
Likes 1	American Municipal Power, 5, Ritts Amy
Dislikes 0	
Response	
Thank you for your comment, this change has been made.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	
Document Name	
Comment	
Duke Energy supports EEI's comments and thanks the Drafting Team for their work.	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
Alliant Energy supports comments submitted by MRO NSRF	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment, please see response to MRO NSRF.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
James Keele - Entergy - 3	
Answer	
Document Name	
Comment	
As Long as Dial-up is not in scope the new requirements for CIP-003-A can be implemented.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Part 3.2 of Attachment 1 for authentication of dial-up were not materially changed as part of this project. The modifications that were made to Part 3.2 from CIP-003-9 were in formatting only. Changes or exclusion of requirement for dial-up are outside the scope of the approved SAR for this project.	
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	
Document Name	
Comment	
Tacoma Power supports SMUD's comments on the technical rationale changes.	
Likes 1	American Municipal Power, 5, Ritts Amy
Dislikes 0	
Response	
Thank you for your comment, please see response to SMUD.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	
Document Name	2023-04 Unofficial Comment Form Additional Ballot_NSRF FINAL_20240306.docx
Comment	
The High VSL column for R2 regarding electronic access (Section 3) contains a typo at the end of the second paragraph. "Section 2" should read "Section 3".	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	

Response	
Thank you for your comment, this change has been made.	
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	
Thank you for your response.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	
Document Name	
Comment	
As Long as Dial-up is not in scope the new requirements for CIP-003-A can be implemented.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Part 3.2 of Attachment 1 for authentication of dial-up were not materially changed as part of this project. The modifications that were made to Part 3.2 from CIP-003-9 were in formatting only. Changes or exclusion of requirement for dial-up are outside the scope of the approved SAR for this project.	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE recommends revising Requirement Part 3.1 from “shall implement a control(s) that” to “shall implement one or more controls that.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, this change has been made.	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	

Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Matthew Jaramilla, 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	
Salt River Project still has concerns on how CIP-003 is written for low impact requirements to 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	
Thank you for your comments. The DT 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.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	

Document Name	
Comment	
BC Hydro appreciates the drafting team's efforts and the opportunity to comment, and offers the following suggestion. BC Hydro suggests included in the Technical Rationale more pertinent use cases and examples to clarify the language used in the revised standards. Specifically the use of 'operational, procedural or technical' methods mentioned in the revised CIP-003 standard Attachment 2 Section 3.5 and 3.6.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT provided several technical options in Attachment 2 and in the Technical Rationale document.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	
Document Name	
Comment	
TVA does not agree with the inappropriate scaling of Medium and High controls to BCAs at Low assets. If additional requirement are scaled to Low BCAs, TVA recommends NERC identify Low BCS in the applicability of the CIP-004 - CIP-013 requirements instead of extending CIP-003 R2 to apply the same requirements to Lows.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT notes that medium and high impact standards currently exist for remote access. The DT also notes that the required cyber security program for lows is not generally as strict or comprehensive as that for medium or high impact and also	

attempts to account for a wide diversity of entities that may have only low impact BCS. Medium and high 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 DT 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. Additionally, the DT asserts that this is beyond the scope of the SAR. 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.	
Dania Colon - Orlando Utilities Commission - 5	
Answer	
Document Name	
Comment	
TVA does not agree with the inappropriate scaling of Medium and High controls to BCAs at Low assets. If additional requirements are scaled to Low BCAs, TVA recommends NERC identify Low BCS in the applicability of the CIP-004 - CIP-013 requirements instead of extending CIP-003 R2 to apply the same requirements to Lows.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT notes that medium and high impact standards currently exist for remote access. The DT also notes that the required cyber security program for lows is not generally as strict or comprehensive as that for medium or high impact and also attempts to account for a wide diversity of entities that may have only low impact BCS. Medium and high 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 DT 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. Additionally, the DT asserts that this is beyond the scope of the SAR. 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.

TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	
Document Name	
Comment	

SIGE appreciates the work of the drafting team to address previous feedback provided for CIP-003-A Technical Rationale. SIGE suggests the following changes in order to qualify the type of access that is being addressed by this standard. The use of the verbiage "user-initiated instance of electronic access" could easily be interpreted as any user log-in. The act of a user logging into a local HMI at a substation is technically a "user-initiated instance of electronic access ". The suggested changes are intended to mimic the Interactive Remote Access term as defined in the NERC Glossary of terms, while not making any reference to an ESP.

Section 3.1.3

This is a new cyber security control outlined in the SAR, which requires entities to implement controls to authenticate users when permitting (allowing) each instance of **user-initiated instance of** electronic remote access, **not including system-to-system process communications,** to networks containing low impact BES Cyber Systems. The intent is at the time any access to the "network containing low impact BES Cyber Systems" is being permitted, the remote user is already authenticated. Figure 3 below depicts a situation where the authentication of the remote user is occurring after the user already has access to the "network containing LIBCS" as the authentication servers are on the same network with the LIBCS. The firewall in this scenario allows the user through to the network on which the LIBCS reside before the user is authenticated.

The intention of "each instance" phrase is meant to include the initial authorization and all subsequent re-connection instances of **user-initiated instance of electronic remote access, not including system-to-system process communications,** to the network. If there is a

collection of sub-networks or Cyber Assets within the network containing LIBCS, then multiple re-authentications at those levels would not be required. This control mitigates the risk of unauthenticated user access to networks on which LIBCS reside.

Section 3.1.4 contains an incorrect reference to Figure 4. The correct reference should be Figure 5.

Section 3.1.4

This is a new cyber security control outlined in the SAR. The objective of Attachment 1, Section 3.1.4 is for entities to protect the user authentication information (e.g., username, password, multi-factor authentication (MFA) information, session token, etc.) while in transit between the remote user's Cyber Asset and either the asset containing the LIBCS or the entity's authentication system used to meet Section 3.1.3. The intent is not to specify authentication directly to a particular device, but to allow for entities that desire to use an existing compliant CIP-005 Requirement R2 Intermediate System or similar architecture for access to networks containing LIBCS as well. For example, Figure 4 below depicts authentication at the boundary of the asset containing a LIBCS. In this example, the authentication server and jump host are on a different network than the "network containing LIBCS", making it uniquely different from Figure 3 above.

Figure 5 depicts an example of protected authentication at a central intermediate system before accessing a network containing a LIBCS. This protection mitigates the unintended disclosure of authentication information for remote access of LIBCS.

Section 3.1.5

The objective of Section 3.1.5 is to maintain the original language used in CIP-003-9, Section 6.1, as much as possible. One or more method(s) can be identified as part of this electronic access control. Entities must determine **user-initiated instances of vendor electronic remote access, not including system-to-system process communications**, where permitted, to their low impact BES Asset(s) and/or LIBCS. Such visibility increases an entity's ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular **user-initiated instance of vendor electronic remote access, not including system-to-system process**.

Section 3.1.6

The objective of Section 3.1.6 is to maintain the original language used in CIP-003-9, Section 6.2, as much as possible. One or more method(s) can be identified as part of this electronic access control. Entities must have the ability to disable **user-initiated instances of**

vendor electronic remote access, not including system-to-system process communications, where permitted, for any basis the entity may choose and to prevent security events and propagation of potential malicious communications which may degrade or have adverse effects upon the entity's assets containing LIBCS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. These changes were made to clarify that 3.1.3 and 3.1.4 only apply to user based electronic access. The DT has chosen not to implement these changes as 3.1.5 and 3.1.6 are intended to capture both user based and system to system electronic access. This terminology was taken from the currently approved version of CIP-003-9 Attachment 1 section 6, and as there have been no material changes made to this requirement language, this DT is interested in preserving the associated language. The Technical Rationale has been updated to correctly reference the figures.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	
Document Name	
Comment	
Black Hills Corporation agrees with EEI's comments which request clarification around VPN tunnels and 3rd party authentication. (EEI comments included below) EEI proposes clarification in the Technical Rationale regarding the use of VPN tunnels as a permanent connection between OEMS and/or continuous monitoring vendors who use an HMI to remotely connect to an entity SCADA system to remotely maintain in-scope sites in the context of compliance with Attachment 1, R3, Part 3.1.3. As an example, wind farms can be maintained remotely by the OEM and/or have a continuous monitoring vendor (third-party) using HMIs remotely connected to the SCADA system via VPN tunnel. The VPN tunnel is typically established between a switch or firewall at the wind farm and a similar device at the third-party location. An HMI is set up at the third-party location. VPN tunnels are generally configured to	

connect automatically using pre-established authentication mechanisms. Once a VPN tunnel is formed it is a connection between the OEM and/or continuous monitoring vendor and the SCADA system for the vendor to manage the turbines. In this scenario, discussion in the Technical Rationale about an entity's ability to comply with Attachment 1, R3, Part 3.1.3. would be beneficial because third-party authentication would take place at the HMI and/or SCADA system devices, and the entity would not be in control of each user-initiated instance of electronic access because they occur on the third-party vendor's side of the VPN tunnel. Clarification could include discussion of this scenario in the context of Interactive Remote Access (IRA), and/or what is meant by "user-initiated instance of access to a network containing." EEI believes this change to the Technical Rationale document could be made without a substantive change requiring another ballot.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Richard Jackson - U.S. Bureau of Reclamation - 1	

Answer	
Document Name	
Comment	
Reclamation recommends when adjusting CIP-003 that changes first be made to Medium and High impact standards. CIP-003 should mirror higher impact requirements but at an equal to or less restrictive level.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT notes that medium and high impact standards currently exist for remote access. The DT also notes that the required cyber security program for lows is not generally as strict or comprehensive as that for medium or high impact and also attempts to account for a wide diversity of entities that may have only low impact BCS. Medium and high 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 DT 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. Additionally, the DT asserts that this is beyond the scope of the SAR.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	
Southern Company is in agreement with EEI comments.	
Likes 0	

Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Carver Powers - Utility Services, Inc. - 4	
Answer	
Document Name	
Comment	
Provide guidance on how a system similar to an Intermediate System could be used to meet 3.1.3 and 3.1.4. Technical guidance diagrams. The information in figure 4 should be included in the diagram for figure 1 and figure 2. Figure 4 provides confusion because it does not meet the criteria listed in 3.1.1 and 3.1.2. Figure 5 is not referenced in any of the guidance and is unclear if there is user authentication information between the jump host and the BES Cyber System.	

Several projects were/are modifying CIP-003 in parallel (2016-02, 2020-03 and 2023-04) and a different approach is used in dealing with the previous Technical Rationale content. For example, in Project 2023-04, hyperlinks to the previous TRs are added in the document, whereas in 2016-02, information from the previous TRs is kept and information was added related to the 2016-02 changes. Furthermore, the recently approved CIP-003-9 TR filed with the 2020-03 project contained only 8 pages from the initial 32 pages. These 8 pages consisted only the changes regarding the -9 version. In summary, three different projects modifying the CIP-003 and its TR with three different approaches. As a general comment, it would be helpful to the industry for the NERC SDTs to choose a way going forward that is applied across all NERC projects. In the case of the TR in this project, we suggest keeping one TR that includes the previous versions of the TR, as was done in the 2016-02 project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has made changes to clarify the Technical Rationale and believes the changes made address your comments. The TR written by 2016-02 contains the historical TR for previous versions of the standard. Prior to final ballot, the DT for 2023-04 will combine both TR files and retain the historical TR.	
Jamie Monette - Jamie Monette On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Jamie Monette	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	

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	
Thank you for your response.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	
Document Name	
Comment	
Jump Server comment. Technical guidance diagrams. Within the Technical Guidance diagrams there is a concern on Figure 3 and Figure 4 concerning if both diagrams are approved configurations or if figure 3 is an incorrect configuration and Figure 4 is an appropriate configuration. Additionally, in Figure 4 there needs to be a key for the line colors and a DMZ designation. Several projects were/are modifying CIP-003 in parallel (2016-02, 2020-03 and 2023-04) and a different approach is used in dealing with the previous Technical Rationale content. For example, in Project 2023-04, hyperlinks to the previous TRs are added in the document, whereas in 2016-02, information from the previous TRs is kept and information was added related to the 2016-02 changes. Furthermore, the recently approved CIP-003-9 TR filed with the 2020-03 project contained only 8 pages from the initial 32 pages. These 8 pages consisted only the changes regarding the -9 version. In summary, three different projects modifying the CIP-003 and its TR with three different approaches. As a general comment, it would be helpful to the industry for the NERC SDTs to choose a way going forward that is	

applied across all NERC projects. In the case of the TR in this project, we suggest keeping one TR that includes the previous versions of the TR, as was done in the 2016-02 project. We note that according to the proposed texts and considering the current version of CIP-005 for Medium Impact Systems, the level of security required for remote access of Low Impact systems is higher than for that of Medium Impact systems without Control Center. We assume that the future revision of CIP-005 will correct this apparent inconsistency.ma	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has made changes to clarify the Technical Rationale and believes the changes made address your comments. The TR written by 2016-02 contains the historical TR for previous versions of the standard. Prior to final ballot, the DT for 2023-04 will combine both TR files and retain the historical TR. Thank you for your comments. The DT notes that medium and high impact standards currently exist for remote access. The DT also notes that the required cyber security program for lows is not generally as strict or comprehensive as that for medium or high impact and also attempts to account for a wide diversity of entities that may have only low impact BCS. Medium and high 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 DT 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. Additionally, the DT asserts that this is beyond the scope of the SAR.	
Ben Hammer - Western Area Power Administration - 1	
Answer	
Document Name	

Comment	
The High VSL column for R2 regarding electronic access (Section 3) contains a typo at the end of the second paragraph. “Section 2” should read “Section 3”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, this change has been made.	
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	
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) and the MRO NSRF for questions #5.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	

EEI proposes clarification in the Technical Rationale regarding the use of VPN tunnels as a permanent connection between OEMS and/or continuous monitoring vendors who use an HMI to remotely connect to an entity SCADA system to remotely maintain in-scope sites in the context of compliance with Attachment 1, R3, Part 3.1.3.

As an example, wind farms can be maintained remotely by the OEM and/or have a continuous monitoring vendor (third-party) using HMIs remotely connected to the SCADA system via VPN tunnel. The VPN tunnel is typically established between a switch or firewall at the wind farm and a similar device at the third-party location. An HMI is set up at the third-party location. VPN tunnels are generally configured to connect automatically using pre-established authentication mechanisms. Once a VPN tunnel is formed it is a connection between the OEM and/or continuous monitoring vendor and the SCADA system for the vendor to manage the turbines.

In this scenario, discussion in the Technical Rationale about an entity's ability to comply with Attachment 1, R3, Part 3.1.3. would be beneficial because third-party authentication would take place at the HMI and/or SCADA system devices, and the entity would not be in control of each user-initiated instance of electronic access because they occur on the third-party vendor's side of the VPN tunnel.

Clarification could include discussion of this scenario in the context of Interactive Remote Access (IRA), and/or what is meant by "user-initiated instance of access to a network containing."

EEI believes this change to the Technical Rationale document could be made without a substantive change requiring another ballot.

Likes 1	Sempra - San Diego Gas and Electric, 5, Wright Jennifer
Dislikes 0	

Response

Thank you for your comments. Changes have been made to clarify these points in the Technical Rationale.

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	
Document Name	

Comment

We operate within a geographical region characterized by limited access of local academic enrichment opportunities for young professionals in cybersecurity. Moreover, this project will require significant technical effort, substantial capital investment, and the augmentation of staffing resources.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. 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 DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	
Document Name	
Comment	
Dominion Energy supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	

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	
Thank you for your response.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	
Document Name	

Comment
LS Power Development agrees with comments submitted by EEL. Thank you for the opportunity to comment.

Likes 0	
Dislikes 0	

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

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

Answer	
Document Name	

Comment
Jump Server comment. Technical guidance diagrams. Within the Technical Guidance diagrams there is a concern on Figure 3 and Figure 4 concerning if both diagrams are approved configurations or if figure 3 is an incorrect configuration and Figure 4 is an appropriate configuration. Additionally, in Figure 4 there needs to be a key for the line colors and a DMZ designation. Several projects were/are modifying CIP-003 in parallel (2016-02, 2020-03 and 2023-04) and a different approach is used in dealing with the previous Technical Rationale content. For example, in Project 2023-04, hyperlinks to the previous TRs are added in the document, whereas in 2016-02, information from the previous TRs is kept and information was added related to the 2016-02 changes. Furthermore, the recently approved CIP-003-9 TR filed with the 2020-03 project contained only 8 pages from the initial 32 pages. These 8 pages consisted only the changes regarding the -9 version. In summary, three different projects modifying the CIP-003 and its TR with three different approaches. As a general comment, it would be helpful to the industry for the NERC SDTs to choose a way going forward that is applied across all NERC projects. In the case of the TR in this project, we suggest keeping one TR that includes the previous versions of the TR, as was done in the 2016-02 project.

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Changes have been made to clarify the Technical Rationale. The SDT believes the changes made address your comments. The TR written by 2016-02 contains the historical TR for previous versions of the standard. Prior to final ballot, the DT for 2023-04 will combine both TR files and retain the historical TR.	
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 and dedication to this project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is responding in alignment with the comments from the EEI.	
Likes 0	
Dislikes 0	

Response	
Thank you for the comment, please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is responding in alignment with the comments from the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	

Answer	
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to NPCC Regional Standards Committee.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
See EEI Comments	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
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 language allows greater flexibility in determining the location of detection compared to the SDT's specification of "for both inbound and outbound electronic 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 the border of the low-impact asset.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. 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 has made further revisions in Section 3 to clarify.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Mohamed Derbas - Sempra - San Diego Gas and Electric - 1	

Answer	
Document Name	
Comment	
SDG&E supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	

End of Report