Comment Report

Project Name:	2016-02 Modifications to CIP Standards | CIP-003-7, Implementation Plan, and definiton of LERC
Comment Period Start Date:	7/25/2016
Comment Period End Date:	9/6/2016
Associated Ballots:	2016-02 Modifications to CIP Standards CIP-003-7 Implementation Plan IN 1 OT 2016-02 Modifications to CIP Standards CIP-003-7 IN 1 ST 2016-02 Modifications to CIP Standards CIP-003-7 Non-binding Poll IN 1 NB 2016-02 Modifications to CIP Standards Low Impact External Routable Communication | New Term/Definition IN 1 DEF

There were 81 sets of responses, including comments from approximately 76 different people from approximately 68 companies representing 9 of the Industry Segments as shown in the table on the following pages.

Questions

1. Definition: The SDT replaced the term *Low Impact External Routable Connectivity* with *Low Impact External Routable Communication (LERC)* and revised the definition such that it is relevant to the type of communication that occurs crossing the boundary of the BES asset that contains the low impact BES Cyber Systems. This more clearly aligns with the output of CIP-002-5.1 Requirement R1, Part 1.3. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

2. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 2 Physical Security Controls to reflect the retirement of LEAP. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

3. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 3 Electronic Access Controls to require entities to implement electronic access control(s) for LERC, if any, to permit only necessary electronic access to low impact BES Cyber System(s). Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

4. Measure M2: The SDT revised the complementary language of CIP-003-6, Attachment 2, Sections 2 and 3 to make the evidential language of the Measure consistent with the revised requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides example diagrams that illustrate various electronic access controls at a conceptual level. Do you agree with the content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

6. Implementation Plan: The SDT revised the Implementation Plan such that it establishes a single effective (compliance) for the revisions made to Sections 2 and 3 of Attachment 2 in CIP-003, which will be the later of September 1, 2018 or the first day of the first calendar quarter that is nine (9) calendar months after the effective date of the applicable governmental authority's order approving the standard and NERC Glossary term, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If not, please provide the basis for your disagreement and an alternate proposal.

7. If you have additional comments on the proposed revisions to address the FERC directive regarding the LERC definition that you have not provided in response to the questions above, please provide them here.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Chris Gowder	Chris Gowder		FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC
					Lynne Mila	City of Clewiston	4	FRCC
					Javier Cisneros	Fort Pierce Utility Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Stan Rzad	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steve Lancaster	Beaches Energy Services	3	FRCC
					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Mark Brown	City of Winter Park	4	FRCC

					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	9	FRCC
Public Service Enterprise Group	Christy Koncz	1,3,5,6	NPCC,RF	PSEG	Tim Kucey	PSEG - PSEG Fossil LLC	5	RF
					Karla Jara	PSEG - Energy Resources and Trade LLC	6	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co.	1	RF
					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co	3	RF
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
SERC Reliability Corporation	David Greene	10	SERC	SERC CIPC	Bill Peterson	SERC RRO	10	SERC
					Mike Hagee	SERC RRO	10	SERC
					SERC CIPC	Various	1,2,5,9	SERC
MRO	Emily Rousseau	1,2,3,4,5,6	MRO	MRO-NERC Standards Review Forum (NSRF)	Joe Depoorter	Madison Gas & Electric	3,4,5,6	MRO
					Chuck Wicklund	Otter Tail Power Company	1,3,5	MRO
					Dave Rudolph	Basin Electric Power Cooperative	1,3,5,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Jodi Jenson	Western Area Power Administration	1,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Mahmood Safi	Omaha Public Utility District	1,3,5,6	MRO

					Shannon Weaver	Midwest ISO Inc.	2	MRO
					Mike Brytowski	Great River Energy	1,3,5,6	MRO
					Brad Perrett	Minnesota Power	1,5	MRO
					Scott Nickels	Rochester Public Utilities	4	MRO
					Terry Harbour	MidAmerican Energy Company	1,3,5,6	MRO
					Tom Breene	Wisconsin Public Service Corporation	3,4,5,6	MRO
					Tony Eddleman	Nebraska Public Power District	1,3,5	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
Joe McClung	Joe McClung		FRCC	JEA Voters	Ted Hobson	JEA	1	FRCC
					Ted Hobson	JEA	1	FRCC
					Garry Baker	JEA	3	FRCC
					Garry Baker	JEA	3	FRCC
					John Babik	JEA	5	FRCC
					John Babik	JEA	5	FRCC
Con Ed - Consolidated Edison Co. of New York	Kelly Silver	1	NPCC	Con Edison	Kelly Silver	Con Edison Company of New York	1,3,5,6	NPCC
					Edward Bedder	Orange and Rockland Utilities	NA - Not Applicable	NPCC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation	6	SERC

						and Energy Marketing		
BC Hydro and Power Authority	Patricia Robertson	1		BC Hydro	Patricia Robertson	BC Hydro and Power Authority	1	WECC
					Venkataramakrishnan Vinnakota	BC Hydro and Power Authority	2	WECC
					Pat G. Harrington	BC Hydro and Power Authority	3	WECC
					Clement Ma	BC Hydro and Power Authority	5	WECC
Seattle City Light	Paul Haase	1,3,4,5,6	WECC	Seattle City Light	Pawel Krupa	Seattle City Light	1	WECC
					Dana Wheelock	Seattle City Light	3	WECC
					Hao Li	Seattle City Light	4	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Bud Freeman	Seattle City Light	6	WECC
					Paul Haase	Seattle City Light	1,3,4,5,6	WECC
					Ginette Lacasse	Seattle City Light	1,3,4,5,6	WECC
PPL - Louisville Gas and Electric Co.	Robert Tallman	3,5,6	RF,SERC	LG&E and KU Energy	Bob Tallman	LG&E and KU Energy	3,5,6	SERC
					Charlie Freibert	LG&E and KU Energy	3	SERC
					Dan Wilson	LG&E and KU Energy	5	SERC
					Linn Oelker	LG&E and KU Energy	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,10	NPCC	RSC no NextEra	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC

					Wayne Sipperly	New York Power Authority	4	NPCC
					David Ramkalawan	Ontario Power Generation	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	UI	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
					Brian Shanahan	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					MIchael Forte	Con Edison	1	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Kathleen M. Goodman	ISO-NE	2	NPCC
					Kelly Silver	Con Edison	3	NPCC
					Peter Yost	Con Edison	4	NPCC
					Brian O'Boyle	Con Edison	5	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Sean Bodkin	Dominion	4	NPCC
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE

					Ronald Bender	Nebraska Public Power District	1,3,5	SPP RE
					Tara Smith	Sunflower Electric	1	SPP RE
					Steven Keller	Southwest Power Pool Inc.	2	SPP RE
					Louis Guidry	Cleco	1,3,5,6	SPP RE
Santee Cooper	Shawn Abrams	1		Santee Cooper	Tom Abrams	Santee Cooper	1	SERC
					Rene' Free	Santee Cooper	1	SERC
					Chris Jimenez	Santee Cooper	1	SERC
					Troy Lee	Santee Cooper	1	SERC
					Bob Rhett	Santee Cooper	5	SERC
Oxy - Occidental Chemical	Venona Greaff	7		Oxy	Venona Greaff	Occidental Chemical Corporation	7	SERC
					Michelle D'Antuono	Ingleside Cogeneration LP.	5	Texas RE
ACES Power Marketing	Warren Cross	1,3,4,5	MRO,RF,SERC,SPP RE,Texas RE,WECC	ACES Standards Collaborators	Brazos Electric Power Cooperative, Inc.	BREC	1,5	Texas RE
					Old Dominion Electric Cooperative	ODEC	3,4	SERC
					Golden Spread Electric Cooperative	GSEC	5	SPP RE
					Prairie Power, Inc.	PPI	1,3	SERC
					Arizona Electric Power Cooperative, Inc.	AEPC	1	WECC
					Hoosier Energy Rural Electric Cooperative, Inc.	HE	1	RF
					Buckeye Rural Electric Cooperative, Inc.	BUCK	4	RF
					Wabash Valley Power Association	WVPA	3	SERC

					East Kentucky Power Cooperative	EKPC	1,3	SERC
					Central Iowa Power Cooperative	CIPCO	1	MRO
					Rayburn Country Electric Cooperative, Inc.	RCEC	3	SPP RE

1. Definition: The SDT replaced the term *Low Impact External Routable Connectivity* with *Low Impact External Routable Communication (LERC)* and revised the definition such that it is relevant to the type of communication that occurs crossing the boundary of the BES asset that contains the low impact BES Cyber Systems. This more clearly aligns with the output of CIP-002-5.1 Requirement R1, Part 1.3. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

John Varnell - Tenaska, Inc. - Tenaska Power Services Co. - 6

Answer	No
Document Name	

Comment

: What is the “Bounder of the BES asset”? I believe this should say “crossing the defind boundery of the BES asset” The word "asset" is also a problem I think it is to broad. I am not sure how to narrow the focus.

Likes 1	Michael Watkins, N/A, Watkins Michael
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

he definition contains two terms that we respectfully suggest should be defined terms as they are fundamental to the meaning of LERC and subsequently critical to meeting compliance requirements of any standards/requirements that use the term.

"BES asset boundary" is used in numerous instances within the standard attachments and it is assumed that it is synonymous with the term "boundary of an asset", which is used in the definition of LERC. What is meant by the term is described in the GTB, "Requirement R2, Attachment 1, Section 3 - Electronic Access Controls". Because there is no correlation between the GTB of the standard and the LERC definition there is no way to understand the term "boundary of an Asset" when reading the LERC definition. The concept of the asset boundary as used in the LERC definition is critical to the meaning of the term LERC and as such it is critical that it be clear and unambiguous. The only way to do that is through the use of a define term or define it within the LERC definition.

"intelligent electronic devices" is used in the definition and in several instances within the GTB of the standard but it is not a common term to the extent that it is unambiguous. We respectfully suggest that the term should be clearly defined as a defined term. The word "intelligent" within the term is very subjective and can be interpreted in many different ways. For example it could be interpreted to mean "artificial intelligence" or it could be interpreted to mean "can perform an action without specific direction". "artificial intelligence implies a very sophisticated level of computing where "can perform an action without specific direction" could be a simple timer.

As both of these terms are paramount to the understanding of the term LERC we suggest that they be appropriatly included as a defined term or defined within the LERC definition.

Likes 0	

Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	No
Document Name	

Comment
The proposed definition raises more ambiguity than the current definition and goes beyond the direction of the FERC order. The definition needs to clearly state whether outbound and inbound communications are being considered and use terminology and structure similar to what is used for other protected measures. Further, physical and electronic characteristics are confused.

Likes 0	
Dislikes 0	

Response

Emily Rousseau - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO-NERC Standards Review Forum (NSRF)	
Answer	No
Document Name	

Comment
The change in definition of LERC will require more documentation about each low impact asset's external communication than what is required for medium impact assets. We would prefer the current definition of LERC (Low Impact External Routable Connectivity) versus the proposed definition. It does not require documentation of electronic access controls if there is no routable connection to low impact BES Cyber Assets.

Likes 0	
Dislikes 0	

Response

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	

Comment
The definition needs clarification as it is vague. It may be necessary to carefully identify inclusions and exclusions (similar to the BES definition). If both are defined, clear identify priority among the inclusions and exclusions. Please note that the term LERC is improperly used throughout the Guidelines and Technical Basis by referring to communications not involving any low impact BES Cyber System as LERC.

The definition includes any routable communication that crosses a BES asset boundary. This definition would encourage adding new requirements for BES assets containing only low impact BES Cyber Assets regulating communication paths into a site unrelated to the BES. For example, if a corporate network is present for local use such as for a maintenance work order system is present, then the low impact BES Cyber Assets are now subject to the requirements of the Standard. As written, even a person walking inside a BES asset boundary with a smartphone having web access would elevate the site to having LERC as the phone utilizes IP. This definition is unworkable.

In practice, the inconsistency between the definition and attachment 1 section 3 potentially adds to confusion on the initial reading of the requirements. Further, the need for 9 example models and 12 pages in the Guidelines and Technical Basis to explain the definition indicates there is a fundamental problem with the approach.

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

Response

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

Answer	No
Document Name	

Comment

1. Regarding the shift to the asset physical boundary for determination of whether LERC exists at the asset:

All the examples provided in the Guidelines and Technical Basis are physical boundaries, such as property or fence lines. Shifting the point of demarcation for LERC to the BES asset physical boundary such as property or fence lines pushes LERC far away in proximity from the BCSs. The resulting shift in focus to LERC will make controlling BCS electronic access more difficult.

In addition, placing LERC at the physical asset boundary means the corresponding infrastructure will likely be maintained by groups who do not currently have the responsibility for electronic access controls for the BCS.

For example: Temporary office trailers are frequently brought onsite to house the additional staff to support large projects. No matter how they are connected, it will be far removed from any BCS impact, but if it crosses the BES asset boundary, it appears LERC would have to be identified and assessed.

The entity suggests the drafting team revise the language to clarify that an inventory or assessment of communications paths to the asset is not required for assets the entity has determined to have LERC.

2. Regarding controls for “Cyber Asset(s) that provide electronic access”:

The Guidelines and Technical Basis states that the “BES asset boundary” is synonymous to the concept of a “logical border” demarcation.

Does the responsible entity have the option to declare the BES asset boundary “closer in” to the BCSs than a perimeter fence, such as declaring a logical border around the asset’s control network, which includes all BCSs, and excludes many non-essential networks, such as an IT owned and operated business network?

The entity suggests the drafting team revise the language to clarify that the entity has the responsibility for determining the appropriate location within the logical infrastructure to implement electronic access controls required by Attachment 1 Section 3.

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

Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	No
Document Name	
Comment	

Seattle appreciates the efforts the Standards Drafting team to address FERC's questions about LERC as expressed in Order 822 but does not agree with the proposed approach.

Modification to LERC definition draws into scope routable communications among non-BES Cyber Systems isolated from BES Cyber Systems or BCS communication networks. For example, as written, LERC would apply to a business network-connected desktop computer at a Low impact location--that by itself is not and has no connection to any BES Cyber System--solely because the routable communications from the non-BES system cross the boundary of the Low impact site. As such, a Low impact asset with BES Cyber Systems that lack any routable connectivity would still have LERC (and thus require the protections of CIP-003-7) if there was a routable business network—or any other routable communications, even presumably a hotspot enabled by a cellphone located outside the asset (site)—present.

This change greatly expands the scope of LERC under the proposed definition. Indeed, in a very real sense, it makes it all but impossible for a low impact asset (site) not to have LERC. This change goes far beyond the request of FERC in Order 822 to address what is meant by “directly” connected and is not warranted nor necessary.

As a possible corrective that restores the scope of LERC to something similar to the present scope, Seattle City Light suggests additional language for the definition of LERC such as “Routable protocol communication AMONG ONE OR MORE BES CYBER SYSTEM(S) that crosses the boundary of an asset containing one or more low impact BES Cyber System(s), excluding…” (CAPITALS indicate additions).

Also, please clarify if LERC is intended to apply to an entire asset (site) or if on a system-by-system basis. The previous definition of LERC clearly applied to individual BES Cyber Systems, in that one BCS at an asset might have LERC and another at the same asset might not have LERC. The new definition, as written, appears to define LERC as a characteristic of the asset (site) as opposed to a characteristic of a cyber system or a BES Cyber System. Seattle City Light recommends clearly stating whichever approach in intended, and strongly prefers language to retain the existing system-based approach. As such, Seattle recommends adding the following sentence at the end to the LERC definition: “THE PRESENCE OR LACK OF LERC IS EVALUATED INDIVIDUALLY FOR EACH BES CYBER SYSTEM EXISTING AT AN ASSET.”

Finally the “Determining Asset Boundary” discussion in the CIP-003-7 Supplemental Material should be revised to clearly state that 1) routable communications on business networks and other non-BES networks having no connection to BES Cyber Systems are excluded from LERC, and that 2) LERC is a property of individual BES Cyber Systems and not a property of an asset (site) as a whole.

Likes 1	Black Hills Corporation, 1, Wingen Wes
Dislikes 0	

Response	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	No
Document Name	
Comment	

We recommend replacing “communication” with “connectivity” because communication may weaken the security of the cyber asset. Securing connectivity protects against all attacks using that network pathway. Only securing against communications path would allow reduced security. Because you can be connected without communicating per the OSI layers. Connectivity and communications are diferent OSI layer, which opens up the possibility of connectivity without communications. This leaves a path for attackers to connect through the asset’s boundary.

Previous definition was more clear and resulted in less burden on Registered Entities. The propsed definition adds administrative burden without adding any reliability benefit to the BES. Additionally designating an entire asset as LERC may rope non-BES Cyber Assets into compliance with potential future Standards aimed at protecting LERC assets.

If proposed definition must stay:

Physical demarcation (asset boundary) for logical controls does not make sense. As written it is too prescriptive; owners should be allowed discretion on boundary. We propose to allow Entities to define their own logical boundary or boundaries within a low impact asset, essentially a low impact ESP (LESP). An LESP would allow an entity the ability to narrow the scope of applied controls and regulation to low impact Cyber Systems, as CIP is intended, without involving systems that have no reliability impact. Additionally an entity that only has many Low Impact Systems would still have the ability to label the whole site as an LESP or Low Impact Security Zone (LISZ). The LESP would not carry over typical requirements of ESPs so use of the term LISZ may avoid confusion.

Alternatively, we suggest adding a clause to the definition such that the cross boundary communication must be associated with the functionality or operability of the low impact Cyber Systems to constitute LERC. This eliminates the issues below that arise with the current proposed definition:

- Wireless communications, which have no impact on low impact BCS (data enabled cell phone), create the existence of temporary LERC. Given the prevalence of mobile phones, it is hard to imagine a substation which does not have LERC at some time.
- Air gapped configurations do not have the same risk profile as networked substations, but both will be labeled as LERC, thereby undermining the signaling impact of a LERC label. It also creates administrative burden with no reliability impact.
- Certain assets which contain low and medium impact BCS may be listed as non-ERC and LERC. This is unnecessarily confusing.

Remove phrase “or vendor proprietary protocol”. This incentives entities to adopt vendor proprietary protocols to avoid compliance obligation. Incentivizing diverse protocols will reduce the ability of entities to use compatible devices for security solutions in the future.

Likes 1	New York State Reliability Council, 10, ADAMSON ALAN
Dislikes 0	

Response

Erika Doot - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

Reclamation is concerned that the proposed LERC definition would encompass corporate network or personal devices that do not monitor or control BES assets, and have no connectivity to BES assets. Reclamation does not believe that all routable devices within the perimeter of BES assets should fall within the scope of CIP standards. Indeed, In the red-line draft for CIP-003-7, the revised standard often uses the term "Cyber Asset" instead of

BES Cyber Asset" which can be an indication that the scope was inadvertently expanded. Reclamation requests that the proposed LERC definition be restricted to include only routable devices which monitor or control BES assets, and which would impact the BES if damaged or compromised.

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

Alternatively, we suggest adding a clause to the definition such that the cross boundary communication must be associated with the functionality or operability of the low impact Cyber Systems to constitute LERC. This eliminates the issues below that arise with the current proposed definition:

- *Wireless communications, which have no impact on low impact BCS (data enabled cell phone), create the existence of temporary LERC. Given the prevalence of mobile phones, it is hard to imagine a substation which does not have LERC at some time.*
- *Air gapped configurations do not have the same risk profile as networked substations, but both will be labeled as LERC, thereby undermining the signaling impact of a LERC label. It also creates administrative burden with no reliability impact.*

Likes 1	New York State Reliability Council, 10, ADAMSON ALAN
Dislikes 0	

Response

Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

I. A primary concern is that the new definition applies to routable communications at a facility that leave that facility (“boundary of the asset”). This is a change from the previous use and definition of LERC, as LERC was previously applied to communications between BES Cyber Assets. This requires the registered entity to focus compliance gathering efforts on non-BES cyber assets with no routable connectivity to BES cyber assets. It is not clear whether this change was intended to include non-BES cyber assets as part of LERC.

II. Another concern is the phrase “time-control functions between non-Control Center BES assets,” the explicit inclusion of “non-Control Center BES assets” does not seem to add any value. There may be cases where time-sensitive protection functions exist between non-Control Center BES assets and Control Center assets.

III. The new definition needs to clarify how the term ‘asset’ is applied, since an asset as stated in CIP-002-5.1, R1.i through R1.vi can mean facilities, components, or systems.

Proposed definition is as follows:

"Routable protocol communication that crosses the boundary of an asset, such as control center, substation, or generating station, containing external routable communications between one or more low impact BES Cyber System(s), excluding communications between intelligent electronic devices used for time mandatory protection or control GOOSE or vendor proprietary protocols."

Likes 0	
Dislikes 0	

Response

Robert Tallman - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name LG&E and KU Energy

Answer	No
Document Name	

Comment

LG&E/KU's concern is based on adding the concept and/or definition of "boundary of an asset" to the LERC definition. While this appears to be more a "PSP-like" definition, LG&E/KU prefer the "demarcation" concept NERC presented in previous lessons learned and FAQs. The draft definition could make it difficult for the Responsible Entities to determine the exact boundary and when doing so, may introduce burdens the SDT is trying to eliminate, due to risk, with Low Impact systems. LG&E/KU understands the SDT desire to keep the "no inventory needed for Low" concept in place however, the administrative burden in the end may be the same. Since most of the facilities (generation plants for example) contain both control LANs and corporate LANs, it will now be necessary to produce both control LAN networks drawings along with corporate LAN network drawings in order to prove the "air gap", where before all that was required were the control LAN documentation. The final concern LG&E/KU has deals with the backhaul networks. In many cases the control LAN and other communication (data, voice, etc.) may be combined by a multiplexer to allow time sequenced priority over a single T1 line. In these cases, the multiplexer just passes the data to the next multiplexer in line and the T1 line could carry both routable and non-routable traffic, thus causing confusion over how to exactly classify this device.

LG&E/KU support most of the EEI comments on this requirement change, however, LG&E/KU would like to see the exemption from 4.2.3.2 included within the definition. NERC had endorsed the concept of creating a "demarcation point" at the Low Impact system to exclude those cyber assets within the communcation network. LG&E/KU suggests the LERC definition be:

"Any electronic routable protocol communcation entering or leaving the BES asset boundary that provides connectivity to Low Impact BES Cyber System(s), excluding communication between: (1) Low Impact BCS located at the same BES asset; (2) Cyber Assets associated with communication networks and data communication links between different BES assets boundaries and/or Electronic Security Perimeters; and (3) intelligent electronic devices used for time Exempt Cyber Systems mandatory protection or control including, but not limited to, IEC 61850 GOOSE or vendor proprietary protocols."

Likes 0	
Dislikes 0	

Response

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

Answer	No

Document Name	

Comment

The proposed revisions to the Low Impact External Routable Connectivity (LERC) definition, retirement of the Low Impact Electronic Access Point (LEAP) and associated changes to the requirements for CIP-003 Attachment 1 Section 2 and 3 represent a significant shift from the currently FERC-approved definitions and requirements. The proposed changes include identifying LERC to non-BES Cyber Assets increasing the scope. Entities are well into their implementation of the approved definitions and requirements. This fundamental shift creates regulatory uncertainty for entities and timing concerns to meet the proposed implementation schedule due to re-work and the volume of assets containing low impact BES Cyber Systems. At best, FERC approval is not likely till near the end of 2017, which will be too late for most entities' budgeting schedules for work to be completed in 2018 if the revised requirements require budget changes. It's not logical to vote yes on the non-binding poll until the requirement language is closer.

Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 1,3, Gresham Darnez
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	No
Document Name	

Comment

We suggest the language: Communication that uses a routable protocol that crosses the boundary of an asset containing one or more low impact BES Cyber System(s), excluding communications between intelligent electronic devices used for time [illegible] non [illegible] Control Center BES assets containing low impact BES Cyber Systems (i.e. IEC 61850 GOOSE or vendor proprietary protocols). We suggest the language: Communication that uses a routable protocol that crosses the boundary of an asset containing one or more low impact BES Cyber System(s), excluding communications between intelligent electronic devices used for time [illegible] Control Center BES assets containing low impact BES Cyber Systems (i.e. IEC 61850 GOOSE or vendor proprietary protocols).

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

The terms associated with low impact electronic access controls should be congruent with the terms for medium and high impact. CenterPoint Energy believes the use of "ERC" should remain External Routable Connectivity. CenterPoint Energy recommends "LERC" to stand for "Low Impact External Routable **Connectivity**" with the following definition:

“The ability to access a low impact BES Cyber System from a Cyber Asset that is outside of its associated BES asset as identified in CIP-002 via a bi-directional routable protocol connection.”

Making this change should address the Commission’s directive as it gets rid of the term “direct” and aligns with the commentary in the Guidelines and Technical Basis section of CIP-003-6. Clarity is provided as this is the same term/concept that has been applied in medium and high impact facilities. It should be a matter of extending this concept to low impact facilities and implementing requirements at an appropriate level based on risk, low.

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6

Answer	No
Document Name	

Comment

Considering the new NERC definition of LERC as “routable communication that crosses the boundary of an asset” in conjunction with Attachment 1 Section 3 Part 3.1 requiring the implementation of “electronic access control(s) for LERC”, these changes could be misinterpreted to mean that access controls are to be performed *at the boundary* of a BES asset since that is a key component of the definition of LERC. It is requested that the SDT add explicit language to the requirement or the Supplemental Material that reduces this risk of misinterpretation, such as, “…although LERC is contingent upon the routable communications crossing the BES Asset boundary, the controls to restrict access for Low Impact BCS with LERC are not required to be implemented at the BES Asset boundary, but instead in a manner that ensures that Applicable Systems are compliant with the control.” Without this explicit language, some entities may interpret the controls as being required at the BES Asset boundary. The existing language may inadvertently increase the scope of assets to include certain devices (i.e. those on the corporate network) that would normally be considered out-of-scope.

Likes 0	
Dislikes 0	

Response

Oliver Burke - Entergy - Entergy Services, Inc. - 1

Answer	No
Document Name	

Comment

I support comments submitted by Entergy's Julie Hall.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	

Texas RE appreciates the SDT's efforts to develop a workable response to FERC's directive in Order No. 822 to provide clarity and eliminate the ambiguity surrounding the term "direct" as it is used in the current definition of Low Impact Routable Connectivity. However, Texas RE is concerned that the SDT's proposed approach to resolving this ambiguity by shifting the focus away from connectivity to communications across an asset boundary is not workable. Moreover, the proposed revisions introduce a number of new terms and concepts that, absent clarification, could result in additional confusion across the industry. Instead, Texas RE recommends that the SDT address FERC's directive by eliminating the distinction between "direct" language from the definition of LERC and adopt familiar concepts from the general definition of External Routable Connectivity (ERC) to the Low Impact Cyber Asset environment.

Texas RE is concerned the proposed LERC definition could be read to exclude serial data communications across an asset boundary. Such serial communications may not be exclusively serial in nature because the serial data could be encapsulated and decapsulated (TCP/IP). As such, the data flow still constitutes bi-directional routable protocol that is within the scope of the general ERC definition. Similarly, Texas RE believes that the LERC definition should capture all bi-directional routable protocols, including serial communications that have been converted to use TCP/IP protocols. This is particularly important for reliability because, in Texas RE's experience, significant amounts of data from relays and RTUs (among other devices) are communicated in this fashion.

Conversely, it is possible to interpret the proposed LERC definition as a significant expansion of the current CIP requirements. In particular, because the proposed definition now focuses on "communications" across an asset boundary, a host of communications could now establish the basis for LERC. For example, a cell phone may pass communication data across an asset boundary, potentially making such devices subject to CIP requirements including electronic access controls.

Finally, the proposed LERC definition introduces a number of new or undefined terms that could cause confusion. Specifically, the proposed definition and supporting attachments use terms such as "assets", "BES asset(s)", "non-Control Center BES assets", "non -BE Boundary" in a potentially confusing manner, particularly in connection with uses in other CIP Standards. For example, CIP-002-5.1, R1 uses the term "assets" where CIP-003-7 uses the term "assets" and "BES asset(s)". Another example, Attachment 1 and 2, both use the term "asset(s)."

In light of these concerns, Texas RE respectfully suggests that the SDT modify its approach to addressing the FERC directive. Specifically, rather than introducing new concepts into the LERC definition, the SDT could address FERC's concerns regarding the use of the term "direct" by eliminating that concept from the LERC definition and instead revising the LERC definition along the lines of the current ERC definition. The ERC is currently defined as: "[t]he ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection." At present, Low Impact BES Cyber Systems currently do not have associated Electronic Security Perimeters. The SDT may wish to consider extending the Electronic Security Perimeter requirement to Low Impact BES Cyber Systems as well. Short of this, however, the SDT should revise the LERC definition to track the ERC definition, but eliminate the ESP concept. For example, LERC could be defined as "[t]he ability to access a BES Cyber Systems from a Cyber Asset that is outside of BES Cyber System's asset boundary via a bi-directional routable protocol connection."

Additionally, Texas RE suggests, under R2, the language that reads "*Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required*"; should be removed. Texas RE considers keeping a list of BES Cyber Assets as best practice and the note discourages it. Texas RE encourages entities to have an inventory of their low impact BES Cyber Systems. This type of evidence would line up properly with Attachment 2 and the Guidelines and Technical Basis for Sections 2 and 3. It does not make good business sense to not have a list associated with an asset inventory. There is not a business manager who would encourage not knowing the level of effort needed to perform a job function and the job function here is reliability. Not having a list is going to extend the amount of effort during an audit for the registered entity and the regional entity staff. This attempt to lower compliance risk is detrimental to reliability. If a company does not maintain an inventory how can it be successful in ensuring that efforts to maintain security of that inventory are complete?

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3

Answer	No
Document Name	

Comment

The change of the definition of LERC to any routable communication that crosses the "BES asset" boundary containing Low Impact BES Cyber Systems will create LERC even where there is no communication with BES Cyber Assets. While this *may* reduce confusion over where there is LERC, it significantly increases the documentation necessary to ensure proper access controls (Physical or Logical Isolation) for netowkrs that have no relation to BES control functionality.

Better would be to limit LERC to the affirmative in relation to communication with a BES Cyber System.

Likes 0	
Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10

Answer	No
Document Name	

Comment

The term "boundary of an asset" used in the definition needs to be better defined as opposed to leaving the interpretation up to the reader. The guidance in the Standard itself offers reasonable suggestions that all appear to extend no further than the physical property boundary of the asset. However, guidance is not binding and left to devise an asset boundary of its own choosing, a Registered Entity potentially could create an unreasonable boundary. The SPP RE suggests that "boundary of an asset" be replaced with "property or fence line of an asset". Alternatively, the definition could incorporate the physical access control boundary as established by Section 2 of Attachment 1 to CIP-003-7 such that any traffic crossing that perimeter would be considered LERC.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

The LERC definition coupled with the CIP-003-7 R2, Attachment 1, Section 3 creates administrative burdens that encourage Responsible Entities and auditors to focus their efforts on compliance evidence for assets that have no connectivity to low impact BES Cyber Systems (“LIBCS”). Understandably, the SDT is looking to address the FERC directive to eliminate the ambiguity caused by the term direct in the LERC definition, while trying to avoid requiring Responsible Entities to list LIBCS. While LERC now has more clarity, it is defined in broader terms that will require more evidence to prove that LIBCS do not communicate over LERC, which could be a substantial burden for entities with large numbers of assets.

The use of “boundary of an asset” is similar to the high and medium impact BES Cyber Systems (“BCS”) ESP concept, which creates similar compliance burdens. The risk-based approach of the CIP Standards is meant to focus security and compliance efforts on the most critical assets, the high and medium impact BCS. Applying a similar concept to the LIBCS may dissolve this risk-based approach and encourages auditors to require lists of LIBCS. However, given diversity among Responsible Entity assets, systems, and security approaches, we think it is important to focus on the security objective.

The security objective is to control electronic access to LIBCS such that only necessary and authorized electronic access is allowed. Proving that this security objective is met can be accomplished in multiple ways and at the site, network, or LIBCS level. For example, here are two approaches:

1) Analyze all external connectivity to the asset to see if there is LERC. If a connectivity path meets the LERC definition, implement and document the electronic access control(s) used to “permit only necessary electronic access” to any LIBCS that may reside within the asset.

2) Analyze all LIBCS or their networks and then implement and document the electronic access control(s) and prove the external connectivity/dial-up to all of them.

For some low impact assets, especially large assets with thousands of LIBCS, the first approach may be more feasible. For others with large numbers of low impact assets, especially those with a higher amount of LERC that does not connect to LIBCS, the second approach may be more feasible. The standard should allow flexibility for entities to use these or other methods for documenting LERC in a way that reduces the documentation burden.

To address these issues as well as the implementation issues mentioned under question 6, EEI encourages the SDT to adopt an approach that allows for both methods. One approach to consider, in addition to removal of LEAP, is also removing the LERC definition and focusing on the security objective in Attachment 1, Section 3. We propose alternative language in our answer to question 3.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Response

Jeffrey Watkins - Jeffrey Watkins On Behalf of: Eric Schwarzrock, Berkshire Hathaway - NV Energy, 5; - Jeffrey Watkins

Answer	No

Document Name	

Comment

NV Energy has concens with the proposed definition change. The proposed changes include identifying LERC to non-BES Cyber Assets increasing the scope. The change in definition of LERC will require more documentation about each low impact asset's external communication than what is required for medium impact assets. This change in scope could potentially be burdensome especially since some entities are well into their implementation of the approved definitions and requirements.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

We recommend replacing "communication" with "connectivity" because communication may weken the security of the cyber asset. Securing connectivity protects against all attacks using that network pathway. Only securing against communications path would allow reduced security. Because you can be connected without communicating per the OSI layers. Connectivity and communications are diferent OSI layer, which opens up the possibility of connectivity without communications. This leaves a path for attackers to connect through the asset's boundary. Otherwise, we agree with the new definition.

The definition contains two terms that we suggest should be defined terms as they are fundamental to the meaning of LERC and subsequently critical to meeting compliance requirements of any standards/requirements that use the term.

"BES asset boundary" is used in numerous instances within the standard attachments and it is assumed that it is synonymous with the term "boundary of an asset", which is used in the definition of LERC. What is meant by the term is described in the Guidelines and Technical Basis, "Requirement R2, Attachment 1, Section 3 - Electronic Access Controls". Because there is no correlation between the Guidelines and Technical Basis of the standard and the LERC definition there is no way to understand the term "boundary of an Asset" when reading the LERC definition. The concept of the asset boundary as used in the LERC definition is critical to the meaning of the term LERC and as such it is critical that it be clear and unambiguous. The only way to do that is through the use of a define term or define it within the LERC definition.

"intelligent electronic devices" is used in the definition and in several instances within the Guidelines and Technical Basis of the standard but it is not a common term to the extent that it is unambiguous. We suggest that the term should be clearly defined as a defined term. The word "intelligent" within the term is very subjective and can be interpreted in many different ways. For example it could be interpreted to mean "artificial intelligence" or it could be interpreted to mean "can perform an action without specific direction". "artificial intelligence implies a very sophisticated level of computing where "can perform an action without specific direction" could be a simple timer.

As both of these terms are paramount to the understanding of the term LERC we suggest that they be appropriatly included as a defined term or defined within the LERC definition.

Previous definition was more clear and resulted in less burden on Registered Entities. The propsed definition adds administrative burden without adding any reliability benefit to the BES. Additionally designating an entire asset as LERC may rope non-BES Cyber Assets into compliance with potential future Standards aimed at protecting LERC assets.

If proposed definition must stay:

Physical demarcation (asset boundary) for logical controls does not make sense. As written it is too prescriptive; owners should be allowed discretion on boundary. We propose to allow Entities to define their own logical boundary or boundaries within a low impact asset, essentially a low impact ESP (LESP). An LESP would allow an entity the ability to narrow the scope of applied controls and regulation to low impact Cyber Systems, as CIP is intended, without involving systems that have no reliability impact. Additionally an entity that only has many Low Impact Systems would still have the ability to label the whole site as an LESP or Low Impact Security Zone (LISZ). The LESP would not carry over typical requirements of ESPs so use of the term LISZ may avoid confusion.

Alternatively, we suggest adding a clause to the definition such that the cross boundary communication must be associated with the functionality or operability of the low impact Cyber Systems to constitute LERC. This eliminates the issues below that arise with the current proposed definition:

· Wireless communications, which have no impact on low impact BCS (data enabled cell phone), create the existence of temporary LERC. Given the prevalence of mobile phones, it is hard to imagine a substation which does not have LERC at some time.

· Air gapped configurations do not have the same risk profile as networked substations, but both will be labeled as LERC, thereby undermining the signaling impact of a LERC label. It also creates administrative burden with no reliability impact.

· Certain assets which contain low and medium impact BCS may be listed as non-ERC and LERC. This is unnecessarily confusing.

Remove phrase “or vendor proprietary protocol”. This incentives entities to adopt vendor proprietary protocols to avoid compliance obligation. Incentivizing diverse protocols will reduce the ability of entities to use compatible devices for security solutions in the future.

Likes 0	
Dislikes 0	

Response

Stephanie Little - APS - Arizona Public Service Co. - 5

Answer	No
Document Name	

Comment

AZPS interprets the proposed revisions to the term *Low Impact External Routable Connectivity* to *Low Impact External Routable Communication* (LERC); such that LERC would be relevant to communication that occurs at the boundary of a BES asset that contains low impact BES Cyber Systems (BCS), rather than at the boundary of the BCS, and, therefore, would encompass all cyber assets within that boundary. As such, AZPS is opposed to requiring LERC at the boundary of a BES asset as it will not only significantly increase the scope of this requirement by encompassing assets that are not identified as BCS, but will also increase the complexity of operational functionality and introduce unnecessary risk to the Bulk Electric System (BES) by not having controls that are localized and focused on the BCS.

Likes 0	

Dislikes 0	

Response

Christy Koncz - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG

Answer	No
Document Name	

Comment

PSEG agrees with and supports EEI's comments.

Likes 1	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

Please consider eliminating LERC as a defined term. The definition of LERC is too broad and will cause confusion regarding the concept of asset “boundary”. In addition, the exclusion of “communication protocols for time-sensitive protection or control functions” presents a reliability risk. Rather than “future-proofing” the requirement, this exclusion permits future cyber security risks for time-sensitive communications. Effective implementation of time-sensitive communications needs some level of security measures in order to ensure reliable real-time communications. At the same time, the Standard should avoid prescribing what electronic access controls are required for time-sensitive communications. The Responsible Entity should have the latitude to decide what protections are necessary based on engineering requirements. The discussion of time-sensitive communications and vendor proprietary protocols should not be part of a defined term and should be moved to Attachment One Section 3 (if the exclusion must be kept) or to the Guidelines.

Attachment 2 Section 3.1 can be written without referring to “LERC”. Please see suggested language in comment for CIP-003-7.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

The new definition causes confusion in that it requires a separate and different process than is required for Medium Impact assets. Consider the process to update documentation for a low impact asset that grows to a medium. Now a completely separate process must be initiated to provide medium impact compliant documentation.

Equally as important, this change will require the inclusion of any BES asset which has a completely isolated and self-contained, non-connected, BES Cyber System and a completely separate administrative or security network. There is no security benefit to be gained and compliance would require a tremendous effort by industry. Some companies may even consider removing IP based administrative or security systems to avoid the compliance burden if there is no other IP connection at particular substations.

The change in definition of LERC will require a great deal of work to research and document. It will probably require even more man hours than what is required for medium impact assets. That documentation doesn't compile itself. It takes engineers and technicians making trips to every asset to document what is there.

We would prefer the current definition of LERC (Low Impact External Routable Connectivity) versus the proposed definition. It does not require documentation of electronic access controls if there is no routable connection to low impact BES Cyber Assets.

We went through a great deal of confusion to finally have a common understanding of External Routable Connectivity, introducing a new term will very likely lead us all through that painful process yet again.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

The new definition causes confusion in that it requires a separate and different process than is required for Medium Impact assets. Consider the process to update documentation for a low impact asset that grows to a medium. Now a completely separate process must be initiated to provide medium impact compliant documentation.

Equally as important, this change will require the inclusion of any BES asset which has a completely isolated and self-contained, non-connected, BES Cyber System and a completely separate administrative or security network. There is no security benefit to be gained and compliance would require a tremendous effort by industry. Some companies may even consider removing IP based administrative or security systems to avoid the compliance burden if there is no other IP connection at particular substations.

The change in definition of LERC will require a great deal of work to research and document. It will probably require even more man hours than what is required for medium impact assets. That documentation doesn't compile itself. It takes engineers and technicians making trips to every asset to document what is there.

We would prefer the current definition of LERC (Low Impact External Routable Connectivity) versus the proposed definition. It does not require documentation of electronic access controls if there is no routable connection to low impact BES Cyber Assets.

We went through a great deal of confusion to finally have a common understanding of External Routable Connectivity, introducing a new term will very likely lead us all through that painful process yet again.

Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	No
Document Name	
Comment	
The proposed revised LERC definition expands the scope for evidence requirements to include connectivity to non-BES Cyber Assets. For example, an entity may not have LERC to the BES Cyber Assets at an asset, but may have LERC to non-BES Cyber Assets. The change in the definition requires entities to identify LERC to non-BES Cyber Assets then provide evidence that this new LERC does not connect to BES Cyber Assets. The scope change creates regulatory uncertainty and issues with completing new work within the proposed implementation schedule. The alternate proposal to retire the LERC definition addresses the FERC directive to address ambiguity of “direct.” The alternate proposal for Attachment 1 Section 3, in response to question 3, captures the obligation for the Responsible Entity. Alternate proposal: Retire the LERC definition, see alternate proposal for question 3.	
Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy supports the comments submitted by Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	

Hydro One supports comments submitted by NPCC RSC.

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4

Answer	No
Document Name	

Comment

The proposed definition as written would allow for the introduction of devices such as smart phones, laptops, tablets, or other devices that if they had connection to a wireless network or some other type of routable connection would be considered LERC and be subject to the applicable sections of CIP-003-7.

The definition does not adequately distinguish between BES Cyber Assets and non-BES Cyber Assets. An added 'bright line' must be included so low impact BES Cyber Systems that have no association, connection or ability to communicate with non-BES Cyber Assets don't drag a "BES asset" into having LERC. For example, with the current definition, a person carrying a smartphone inside the "asset boundary" could create LERC, even though there may be no way for that device to communicate with the BES Cyber Asset. The definition of LERC must include the requirement that the communication pass through an electronic access control device before being permitted to or from the BES Cyber System.

That will result in additional documentation for entities to document those devices that have LERC but are not connected to any BES Cyber System.

Further, the need for 9 example models and 12 pages in the Guidelines and Technical Basis to explain the definition indicates there is a fundamental problem with the approach.

Likes 0	
Dislikes 0	

Response

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters

Answer	No
Document Name	

Comment

JEA supports the LPPC comments.

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

By removing the term "bi directional routable protocol access" from Attachment 1, the SDT has inadvertently caused further vagueness about what protocols are to be included within the requirement. As written this would allow for introduction of devices such as smart phones, laptops, tablets, or other devices that have a connection to a wireless network or some other type of routable connection could be considered LERC and be subject to CIP-003-7.

We propose to modify the definition of LERC to be "Routable protocol communications that crosses the boundary of an asset containing one or more low impact BES Cyber System(s), excluding communications between equipment outside of the site communications demarcation point, or communications between intelligent electronic devices used for time-sensitive protection or control functions between non-Control Center BES assets containing low impact BES Cyber Systems including, but not limited to, IEC 61850 GOOSE or vendor proprietary protocols." Additionally, we suggest modifying R3.1, Section 3, Attachment 1 to be "Implement electronic access control(s) for LERC, if any, to permit only necessary bi directional routable protocol access to low impact BEC Cyber System(s)."; and modify the Guidelines and Technical Basis section Determining LERC, Requirement R2, Attachment 1, Section 3 - Electronic Access Controls.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

In our observation, we noticed that the SDT mentions in its background information the changes to the components of the term ‘LERC’. Additionally, the revision to the definition to provide more clarity for the term (in a different documentation). Also, we’ve observed the term and reference of its definition in the Supplement Guidance Section of the Standard. With that being said, we would suggest to the drafting team to include a section at the beginning of the Standard labed **New or modified Term(s) used in NERC Standards.** This will help the drafting team keep the industry up to date on what new terms have been added or revised in a particular Standard as well as promoting consistency with the formatting of the Standards Development Process.

As for the revision to the definition, we would ask the drafting team does clarity need to be provided on what an ‘intelligent electronic system’ is? Not to be difficult…but aren’t all electronic devices intelligent???. Maybe, the drafting can provide some clarity on that process. Additionally, we would ask that the draft team would they provide clarity on the term ‘boundary’ in the definition to align to the contentds as it states in the guidance documentation.

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	

Comment

FMPA supports the comments of American Public Power Association.

Likes 0	
Dislikes 0	

Response

Jay Barnett - Exxon Mobil - 7

Answer	No
Document Name	

Comment

Although I agree with the flexibility added to the CIP-003, I believe the proposed modification to the definition LERC is too broad. The concern is that entities and auditors could differ on which communications are LERC depending on how they define the boundary of the asset. LERC should be defined such that equipment that doesn't communicate with or impact a BES Cyber Asset is not included within the scope of CIP-003.

Likes 0	
Dislikes 0	

Response

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters

Answer	No

Document Name	
Comment	
JEA supports the LPPC comments.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

N&ST recommends that at a minimum, the definition be revised to clarify what is meant by the “boundary” of an asset. The “CIP-003-7 Supplemental Material” section of CIP-003-7 Draft 1 includes a helpful discussion of the topic (“Determining Asset Boundary”), but N&ST notes that almost since the first version of the CIP Standards became mandatory and enforceable, Responsible Entities have vigorously opposed the so-called practice of “auditing to guidelines.” Absent a clear description of what is meant by “boundary,” the proposed definition of LERC is ambiguous. N&ST recommends that the SDT consider incorporating the draft guideline statement, “The intent is for the Responsible Entity to define the BES asset boundary such that the low impact BES Cyber System(s) that are located at the BES asset are contained within the BES asset boundary,” into the LERC definition.

A second problem with the proposed definition is the fact that, in combination with the proposed revisions to CIP-003-6, it would bring low impact BES Cyber Systems with no network connectivity at all into scope for the requirement to “Implement electronic access controls” (CIP-003-7 Draft 1, Attachment 1, Section 3, Part 3.1) if the BES asset happened to also contain non-BES Cyber Assets with routable connectivity to and from other sites (a corporate network PC, for example). N&ST is certain that entities would prefer to not experience a repeat of the problems caused by the wording of CIP Versions 1-3, which stated entities must have procedures for securing dial-up access to Electronic Security Perimeters and made no allowances for situations where no dial-up access existed. An entity should be required to identify and document that LERC exists at a given BES asset only if one or more low impact BES Cyber Systems at that asset have routable connectivity to and from other sites. The exception for direct, time-sensitive communication between IEDs and similar devices should be maintained.

Finally, N&ST believes that the SDT’s decision to address the problem of what is meant by “direct” communication with low impact BES Cyber Systems by eliminating the word from the definition will fail to put the matter to rest. “LERC Reference Model 4” in the Supplemental Material section of CIP-003-7 Draft 1 reopens the debate by asserting that LERC exists for a serially-connected low impact BES Cyber System that can be reached from offsite via an IP/Serial Converter that is “...continuing the same communications session from device(s) outside the BES asset boundary to the low impact BES Cyber Systems.” N&ST agrees with the view that the use of protocol converters doing nothing more than mapping IP connections to serial connections does in fact establish “direct” routable communication with “target” serial devices, and we believe the LERC definition should say so (along with a hopefully obvious declaration that IP-capable low impact BES Cyber Systems that can themselves initiate or receive IP connection requests have “direct” connectivity).

Likes 0	
Dislikes 0	
Response	

Chris Scanlon - Exelon - 1	
Answer	No
Document Name	

Comment

As currently proposed, the revisions go beyond clarifying the use of “direct” and create additional compliance burdens and regulatory risk without providing a corresponding increase in the reliability benefits. Below are areas of concern:

1. Removal of the filter: The proposal defines all routable electronic access as LERC. This lessens some uncertainty around whether an entity would have to prove the negative (i.e. there would be far fewer instances where an entity would need to prove that LERC does not exist); however, it does so by making everything LERC and expanding the burden to demonstrate a lack of any routable communication over the BES asset boundary. This requires substantial analysis to identify the presence of LERC at asset locations that entities did not need to analyze under the V.6 Standard.

2. The asset boundary: Exelon appreciates the SDT effort to support applying the requirements for Lows at the BES asset level and using the “asset boundary” as a method to define the BES asset and the point at which communication goes from the outside-in or vice versa. In this concept, Exelon appreciates the flexibility given for Responsible Entities to determine the boundary. The GTB discussion is also useful in support of the concept. However, Exelon finds that the “asset boundary” is not necessary to support the security objective and encourages the SDT to consider methods to simplify the approach. In practice, defining an “asset boundary” creates an additional step to the compliance program, a significantly burdensome one for entities with large numbers of BES assets. In response to Question 3 below, there is a proposal that would eliminate the need and use of the “asset boundary” portion of the approach.

3. Absence of communication to a Low impact BES Cyber System: The proposed definition no longer requires that the routable protocol communication from outside the asset containing low impact BES Cyber Systems have any electronic connection (direct or indirect) to a low impact BES Cyber System(s). The new obligation expands the definition beyond the scope of BES assets under the currently approved Version 6 definition. As a result, under the proposed definition, those assets containing low impact BES Cyber Systems with fully separated (air-gapped) low impact BES Cyber Systems would have LERC even if the only routable connection that crossed the “asset boundary” is to a non-BES Cyber System (e.g. a corporate connection). Moreover, in circumstances where all low impact BES Cyber Assets at a BES asset are separated (air-gapped) and therefore not directly or indirectly accessible from outside the asset containing the low impact BES Cyber System, there is no reliability benefit for creating a list of routable connections at the “asset boundary” and it would become a significant administrative effort to document LERC at such assets. This also seems contrary to the fundamental efforts of the CIP standards to focus protections on BES Cyber Systems. To resolve this issue, if the LERC term goes forward (see proposal in response to Question 3 that could eliminate the need for the glossary term), the existence of LERC should require some electronic routable communication connectivity to a low impact BES Cyber System from outside the asset containing the low impact BES Cyber System. To address this concern, the definition could include an exclusion as follows: “excluding routable protocol communication that does not provide a direct or indirect connection to a low impact BES Cyber System from outside the asset boundary.”

Proposal Q1A: Given the concerns above, Exelon proposes the following approach to return to the currently approved LERC definition. The SDT could address the FERC directive by removing the word “direct” from the definition and update the Section 3 Electronic Access Controls requirement as proposed in the response to Question 3.

Additional Note, “C” in LERC and LEAP retirement: Exelon has no objection to changing the “C” in LERC to “Communication” and would support the revision as part of the proposal. “Communication” is a more accurate representation. Retirement of LEAP would also still be appropriate under the SDT proposal and under the proposals outlined in these comments.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	

Comment

Protecting the Bulk Electric System (BES): Sometimes lost in the drafting process is the objective of the NERC Reliability Standards—to guide and provide the framework to reliably operate the BES. That framework includes operations, planning, design, emergency response, and, as in this case, critical infrastructure protection. There are Standards that succeed in ensuring reliable BES operation and there are Standards that consume entities' resources and offer little incremental improvement to reliability. It is through the lens of reliability and cost to implement we offer comments regarding the Proposed LERC definition.

Concern—Boundary of an Asset: The use of "boundary of an asset" is ambiguous, unclear, and has likely unintended consequences.

The term potentially expands applicability to any routable protocol communication that crosses an asset boundary regardless of a connection to a BES Cyber System or not. See CIP -003- 7 Supplemental Material: LERC Reference Model No

The term is silent as to whether it will be applied equally and consistently across an Entity's BES system.

The term, when considered with the glossary terms incorporated by reference, promotes confusion. Specifically, the undefined term, "asset," and glossary term, "BES Cyber Asset," which is incorporated in the definition of BES Cyber System referenced in the proposed LERC term.

Along those lines, the definition of "BES Cyber Asset" incorporates the glossary term, "Facilities." As an example, in an attempt to provide greater certainty around the undefined term, "asset," Entities and the ERO conceivably could look to the glossary term, "Facilities," to interpret the term. We believe such a scenario would bring too many "assets" into scope and go far beyond the intended use of the undefined term, "asset." We recognize such a scenario is unlikely but it, again, highlights the challenge of ambiguity in the proposed definition.

Concern—Boundary of an Asset, Part Two: The phrase, "crossing the boundary of the asset," is ambiguous and unclear whether it is referring only to an electronic boundary and/or a physical boundary.

If boundary includes physical borders, the challenge of interpreting is easily illustrated by the basic plan of a substation.

A substation has multiple points that constitute a physical boundary. For example, the substation property line, its fence, its gate, a control house or houses, and so forth. Then there are the one-offs—does a low impact BES Cyber Asset mounted on a pole or structure in or outside the substation fence line constitute or establish a boundary? The proposed definition does not offer any guidance in that regard.

Concern—Cost to Implement: We expect that the proposed revision will, initially, not greatly impact the industry because of the widespread use of non-routable serial communication between Real-time Units (RTU) and Energy Management Systems (EMS). However, that would change in the future for companies that begin to incorporate routable protocols for communications between RTUs and the EMS, introducing a significant cost and commitment of resources to secure those communications.

When evaluated against the previous LERC definition, the impact becomes apparent. The previous LERC definition was only concerned with "interactive remote access" or people accessing devices inside the low impact substation and remotely modifying their configuration or exercising control over the Facilities. The previous LERC definition excluded machine-to-machine communications using a routable protocol, like communications between RTUs and the EMS.

The proposed definition's scope broadens to include the machine-to-machine communications by including all routable communication except for non-Control Center BES assets.

Unintended Consequence—Delay and Hamper Transformational Change in Substation Communication Infrastructure: The significant cost to implement the compliance obligations created by the proposed LERC definition revisions will incent companies' continued reliance on outdated serial communication standards to defer the implementation costs.

Beyond the cost deferral, companies continuing to rely on analog telecom connections to substations for serial communication will face the hard truth that the principal telecommunication carriers are losing their experienced workforce that are able to maintain the analog systems. As such, the carriers are placing a premium to maintain analog connections. We are aware of a utility that incurred unexpected expense that pushed their costs 44% over budget—representing hundreds of thousands of dollars—just to support their analog system.

The final analysis becomes a business decision—cost to implement against the premium to maintain analog systems, with both being substantial. If the equation favors keeping the analog systems in place, the incentive is diminished to upgrade.

Concern—Security for Security's Sake: The proposed LERC term may very well apply to every BES Facility, establishing a scope so large, Entities would have to devote significant resources to implement and maintain the LERC established assets without a clear or marginal improvement to the reliable operation of the BES.

It is clear in cyber security—it is impossible to plug every hole and often raises the question, should we even try. The statement should not be read as, "why bother;" it highlights Entities' resources are not infinite and there may be more beneficial uses of those resources to favorably impact BES reliability.

Furthermore, there is the concern trolling in low impact weeds without consideration of the risk may actually decrease BES security by misdirecting Entities' attention and causing them not to see fissures and cracks opening in a larger view of the BES Cyber Systems while required to focus on the weeds.

Even recognizing FERC's directive, there is a reason they call them "low impact" assets. We would highlight the need to evaluate the risk; the resources to implement and maintain; and marginal improvement to BES reliability and security. The implications of scope created by the proposed LERC term are significant, material, and likely have unintended consequences.

Concern—Creates Onerous Compliance Tasks: As a corollary to Security for Security's Sake, discussed above, consider the scenario that would, for all intents and purposes, bring every substation into the scope of applicability. The task to install and maintain firewalls and their associated rules under CIP-005-5 would overwhelm most, if not all Entities.

The scenario and its likely impact highlights, there is a reason they call them "low impact" assets. We question whether requiring firewalls at every substation—as reflected in CIP-003-6, Attachment 2, Sections 2 and 3, evidence language—materially improves BES reliability and security.

Concern—Compliance: The proposed LERC term may convert assets to BES Cyber Assets, bringing CIP-002-5.1 into play and an appreciable increase to compliance obligations.

The proposed LERC term may have the unintended consequence of requiring Entities to create comprehensive BES Facility inventories to evidence compliance under CIP-002-5.1. Whether the proposed LERC term or CIP-002-5.1, evidence would be required to support why an asset is or is not a BES Cyber Asset—a "prove the negative" situation. An inventory is the likely path required by auditors to demonstrate compliance.

Proposal

To address our concern regarding the substantial scope of applicability of the proposed LERC definition, we offer the following:

Suggested Modification, delete "containing":

"A routable protocol communication that crosses the boundary of an asset connected to one or more low impact BES Cyber Systems…"

Suggestion

Conceptually, we do not oppose the use of “boundary of asset;” the term needs to either be defined or, at the very least, set out parameters to better establish a manageable scope. We believe our proposed language is a step toward limiting that potential scope of the proposed LERC term.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	No
Document Name	

Comment

We do not agree with these proposed changes.

(1) ACES appreciates the efforts of the SDT with addressing the FERC directive and providing clarity to the LERC definition. However, simply removing ”direct” and replacing “connectivity” with “Communication” generates additional concerns.

(2) Registered Entities have already incurred infrastructure and labor costs to implement various solutions to address the present LERC definition. This include the insertion of unidirectional devices that would intentionally break the communications streams of bi -direc protocol connections. How will these solutions align with the proposed definition?

(3) The SDT proposes to add “Communication” to the LERC definition without providing additional clarification. Does this unintentionally increase the scope of Cyber Assets and BES Cyber Systems? Which of the following Communication protocols are then in scope?

- Computer access control protocols
- Data interchange standards
- Internet protocols
- Network protocols
- Wireless Application Protocol
- XML-based standards

(4) We question how will an entity implement the new LERC definition if they also have External Routable Connectivity? If these two definitions do not align, we believe additional implementation costs and gaps would be created.

(5) The SDT has identified that LERC is an attribute of a “BES asset.” What definition supports this statement? How will Regional Entities consistently apply this definition?

(6) We believe the proposed definition should be modified to clarify the use of an IP Converter as a serial device. We have observed that each Regional Entity has inconsistently applied this use.

Likes 0	
Dislikes 0	

Response

Tim Kucey - PSEG - PSEG Fossil LLC - 5

Answer	No
Document Name	

Comment

PSEG supports comments of EEI and NPCC TFIST

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

NRECA is concerned that the revisions to the LERC definition go significantly beyond addressing the FERC directive to clarify “direct” in the definition. By making everything LERC and requiring the demonstration of a negative (that a connection was never made), this is an added compliance burden without a demonstrated BES reliability benefit. NRECA believes it’s reasonable to require identification and protection demonstration for communication paths that cross the asset boundary and are for BES purposes. However, those communications that have nothing to do with BES communications (i.e., non-BES assets) should be excluded from scope of LERC. Demonstration of an “air-gap” is essentially a requirement to demonstrate a negative (that a connection was never made) and is overly burdensome and does not have a BES reliability benefit. The revisions could make compliance with security for a low impact facility more difficult than at a medium impact facility.

Given NRECA’s concerns, we strongly encourage the SDT to remove the word “direct” from the currently approved LERC definition – this will address FERC’s directive without unnecessarily expanding the scope of LERC beyond the BES. NRECA does not object to changing the “C” in LERC to Communication.

Likes 0	

Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	

Comment
Cowlitz PUD supports the comments as submitted by APPA and Utility Services.

Likes 0	
Dislikes 0	

Response

Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	No
Document Name	

Comment
The revised LERC definition unintentionally draws into scope routable communications between non-BES Cyber Systems and isolated business only communication networks. As written, LERC would apply to all Cyber Assets at a Low impact location if there was a routable business network present. GCPD recommends the following revisions to the proposed LERC definition for clarity. *Routable protocol communication to or from a low impact BES Cyber System that:* • *crosses the boundary of a BES asset containing one or more low impact BES Cyber System(s),* • *does not include communications between intelligent electronic devices used for time* *tions between non-* *Control Center BES assets containing low impact BES Cyber Systems including,* • *is not limited to, IEC 61850 GOOSE or vendor proprietary protocols.* GCPD is also recommending that with a revised definition of LERC as suggested, that CIP-003-7 Supplemental Material be adjusted to reflect and support this revision.

Likes 0	
Dislikes 0	

Response

Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker

Answer	No
Document Name	
Comment	
Generally, we support the LERC definition revisions made, including the replacement of "Connectivity" with "Communication" within the LERC title. However, we do not support a definition that include connections that have nothing to do with the BES. The tasks of (1) identifying and (2) demonstrating protections regarding all communications paths that cross the asset boundary is overly burdensome. We recommend limiting the scope only to those paths that are used for BES communications or to connect to BES Cyber Assets. Thus, it is our position that communications that have nothing to do with BES communications should be excluded from scope. Furthermore, we find no reason to limit the LERC definition to " vendor proprietary protocols." The function of the communication is not to identify a single example of a standard and assume any other examples are proprietary. Thus, we recommend this provision also be excluded.	
Likes 0	
Dislikes 0	
Response	
Oshani Pathirane - Oshani Pathirane On Behalf of: Paul Malozewski, Hydro One Networks, Inc., 1, 3; - Oshani Pathirane	
Answer	No
Document Name	
Comment	
Hydro One Networks Inc. supports the NPCC RSC's comments on this question in its entirety.	
Likes 0	
Dislikes 0	
Response	
Johnny Anderson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Data such as routable protocol communications is routinely transported through low impact substations. Bringing data such as routable protocol communication into scope as a result of the broad definition creates an unnecessary compliance burden. The new definition creates too many complexities and is too broad. As it is written the new definition creates more questions than the clarity it was intended to provide.	
Likes 0	
Dislikes 0	

Response

Michiko Sell - Public Utility District No. 2 of Grant County, Washington - 1	
Answer	No
Document Name	
Comment	

The revised LERC definition unintentionally draws into scope routable communications between non-BES Cyber Systems and isolated business only communication networks. As written, LERC would apply to all Cyber Assets at a Low impact location if there was a routable business network present. GCPD recommends the following revisions to the proposed LERC definition for clarity.

Routable protocol communication ***to or from a low impact BES Cyber System*** *that:*

- *crosses the boundary of* ***a BES*** *asset containing one or more low impact BES Cyber System(s),*
- *does not include communications between intelligent electronic devices used for time* *-se*
  Control Center BES assets containing low impact BES Cyber Systems including,
- *is not limited to, IEC 61850 GOOSE or vendor proprietary protocols.*

GCPD is also recommending that with a revised definition of LERC as suggested, that CIP-003-7 Supplemental Material be adjusted to reflect and support this revision.

Likes 0	
Dislikes 0	

Response

John Bee - Exelon - 3	
Answer	No
Document Name	
Comment	

See Exelon TO Response

Likes 0	
Dislikes 0	

Response

Ruth Miller - Exelon - 5	
Answer	No
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Exelon - 6	
Answer	No
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
NRG supports the comments submitted by NPCC (Ruida Shu on 9/6/16): We recommend replacing “communication” with “connectivity” because communication may weaken the security of the cyber asset. Securing connectivity protects against all attacks using that network pathway. Only securing against communications path would allow reduced security. Because you can be connected without communicating per the OSI layers. Connectivity and communications are diferent OSI layer, which opens up the possibility of connectivity without communications. This leaves a path for attackers to connect through the asset’s boundary. Otherwise, we agree with the new definition. The definition contains two terms that we suggest should be defined terms as they are fundamental to the meaning of LERC and subsequently critical to meeting compliance requirements of any standards/requirements that use the term. "BES asset boundary" is used in numerous instances within the standard attachments and it is assumed that it is synonymous with the term "boundary of an asset", which is used in the definition of LERC. What is meant by the term is described in the Guidelines and Technical Basis, "Requirement R2,	

Attachment 1, Section 3 - Electronic Access Controls". Because there is no correlation between the Guidelines and Technical Basis of the standard and the LERC definition there is no way to understand the term "boundary of an Asset" when reading the LERC definition. The concept of the asset boundary as used in the LERC definition is critical to the meaning of the term LERC and as such it is critical that it be clear and unambiguous. The only way to do that is through the use of a define term or define it within the LERC definition.

"intelligent electronic devices" is used in the definition and in several instances within the Guidelines and Technical Basis of the standard but it is not a common term to the extent that it is unambiguous. We suggest that the term should be clearly defined as a defined term. The word "intelligent" within the term is very subjective and can be interpreted in many different ways. For example it could be interpreted to mean "artificial intelligence" or it could be interpreted to mean "can perform an action without specific direction". "artificial intelligence implies a very sophisticated level of computing where "can perform an action without specific direction" could be a simple timer.

As both of these terms are paramount to the understanding of the term LERC we suggest that they be appropriatly included as a defined term or defined within the LERC definition.

Previous definition was more clear and resulted in less burden on Registered Entities. The proposed definition adds administrative burden without adding any reliability benefit to the BES. Additionally designating an entire asset as LERC may rope non-BES Cyber Assets into compliance with potential future Standards aimed at protecting LERC assets.

If proposed definition must stay:

Physical demarcation (asset boundary) for logical controls does not make sense. As written it is too prescriptive; owners should be allowed discretion on boundary. We propose to allow Entities to define their own logical boundary or boundaries within a low impact asset, essentially a low impact ESP (LESP). An LESP would allow an entity the ability to narrow the scope of applied controls and regulation to low impact Cyber Systems, as CIP is intended, without involving systems that have no reliability impact. Additionally an entity that only has many Low Impact Systems would still have the ability to label the whole site as an LESP or Low Impact Security Zone (LISZ). The LESP would not carry over typical requirements of ESPs so use of the term LISZ may avoid confusion.

Alternatively, we suggest adding a clause to the definition such that the cross boundary communication must be associated with the functionality or operability of the low impact Cyber Systems to constitute LERC. This eliminates the issues below that arise with the current proposed definition:

- Wireless communications, which have no impact on low impact BCS (data enabled cell phone), create the existence of temporary LERC. Given the prevalence of mobile phones, it is hard to imagine a substation which does not have LERC at some time.
- Air gapped configurations do not have the same risk profile as networked substations, but both will be labeled as LERC, thereby undermining the signaling impact of a LERC label. It also creates administrative burden with no reliability impact.
- Certain assets which contain low and medium impact BCS may be listed as non-ERC and LERC. This is unnecessarily confusing.

Remove phrase “or vendor proprietary protocol”. This incentives entities to adopt vendor proprietary protocols to avoid compliance obligation. Incentivizing diverse protocols will reduce the ability of entities to use compatible devices for security solutions in the future.

Likes 0	
Dislikes 0	

Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	2016 02 BPA_No LERC examples_20160906.pdf
Comment	

From FERC Order 822 paragraph 73: “The Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term “direct” as it is used in the proposed definition.”

While BPA agrees that the proposed definition more clearly aligns with the output of CIP-002-5.1 Requirement R1, Part 1.3, BPA believes this changes the focus from device level language to asset level and vastly increases the number of devices that will be subject to compliance. BPA believes this does not improve security commensurate with the increased burden of compliance.

The change from device level to asset level without regard for connections to BES Cyber Systems will vastly increase the number of assets subject to compliance. At BPA, we estimate that the number of Low Impact assets requiring electronic access controls will increase dramatically. Most of these would require extraneous documentation and tracking for communication that was never intended to be addressed by CIP requirements (e.g., corporate network going to into substations without any access to BES equipment).

Proposal: In order to resolve FERC’s concerns about the ambiguity surrounding the word “direct”, BPA proposes that the new definition be modified to better reflect CIP goals. Some of the following language may prove useful in discussions:

“Routable protocol communication, crossing the boundary of an asset containing one or more low impact BES Cyber System(s), capable* of modification of a BES Cyber System”

*Add to Technical Guidance: “Capable” should not include zero-day attacks, software bugs, etc.

“Routable protocol communication that crosses the boundary of an asset containing one or more low impact BES Cyber System(s), unless all BES Cyber Systems are physically air-gapped from the routable protocol…”

Additional models to show LERC/no LERC examples may be helpful (see attached pdf.)

The exclusion segment is difficult to understand:

- In their FAQ at http://www.nerc.com/pa/CI/tpv5impmntnstdy/CIPV5_FAQs_Consolidated_Oct2015_Oct_13_2015.pdf the authors identify IEC 61850 as “an ethernet based standard” that “can be mapped to a number of protocols.” They acknowledge that some of these protocols are routable and some are not. The proposed LERC language exempting IEC 61850 GOOSE is confusing: If they’re referring to the GOOSE protocol, which is defined in IEC 61850-8-1, it is a layer 2 protocol and is not routable. On the other hand, if they are referring to R-GOOSE, which is defined in IEC TR 61850-90-5, it is a layer 3 protocol and is routable. BUT, the name of the protocol is “R-GOOSE”, not “GOOSE”. LERC’s exemption would be much clearer if (1) it didn’t mention IEC 61850 at all, or (2) if it named R-GOOSE specifically, or (3) if it exempted the entire suite of IEC 61850 protocols used for time-sensitive protection and control functions.
- Furthermore, the exclusion is confused by conflicting phrases “excluding” and “including” within the same sentence. If the examples are kept, the exclusion could be broken into a separate sentence for clarity.

Proposed language:

- Suggestion 1 (preferred): “, excluding communications between intelligent electronic devices used for time functions between non -sensi -Control Center BES ass

- Suggestion 2: “This definition excludes communications between intelligent electronic devices used for time functions between non limited to, IEC 61850 or proprietary protocols.”

Or

- “…excludes communications between intelligent electronic devices used for time Control Center BES assets containing low impact BES Cyber Systems, regardless of the protocol, such as, but not limited to, IEC 61850 R-GOOSE or proprietary protocols.”

Likes 0	
Dislikes 0	

Response

Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

Modification to LERC definition inadvertently draws into scope routable communications among non-BES Cyber Systems isolated from BES Cyber Systems or BCS communication networks. For example, as written, LERC would apply to a business network-connected desktop computer at a Low impact location--that by itself is not and has no connection to any BES Cyber System--solely because the routable communications from the desktop cross the boundary of the Low impact site. As such, a Low impact asset with BES Cyber Systems that lack any routable connectivity would still have LERC (and thus require the protections of CIP-003-7) if there was a routable business network present. This expansion of scope to include business networks does not appear to be intentional, and greatly expands the scope of LERC under the proposed definition. As a corrective, Seattle City Light suggests additional language for the definition of LERC such as “Routable protocol communication AMONG ONE OR MORE BES CYBER SYSTEM(S) that crosses the boundary of an asset containing one or more low impact BES Cyber System(s), excluding…” (CAPITALS indicate additions).

Also, please clarify if LERC is intended to apply to an entire asset (site) or if on a system-by-system basis. The previous definition of LERC clearly applied to individual BES Cyber Systems, in that one BCS at an asset might have LERC and another at the same asset might not have LERC. The new definition, as written, appears to define LERC as a characteristic of the asset (site) as opposed to a characteristic of a cyber system or a BES Cyber System. Seattle City Light recommends clearly stating whichever approach in intended, and strongly prefers language to retain the existing system-based approach. As such, Seattle recommends adding the following sentence at the end to the LERC definition: “THE PRESENCE OR LACK OF LERC IS EVALUATED INDIVIDUALLY FOR EACH BES CYBER SYSTEM EXISTING AT AN ASSET.”

Finally the “Determining Asset Boundary” discussion in the CIP-003-7 Supplemental Material should be revised to clearly state that 1) routable communications on business networks having no connection to BES Cyber Systems are excluded from LERC, and that 2) LERC is a property of individual BES Cyber Systems and not a property of an asset (site) as a whole.

Likes 0	
Dislikes 0	

Response

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray

Answer	No

Document Name	
Comment	
Changing the definition to include “Communication” instead of “Connectivity” and following the basis behind this proposal, all substations containing Low Impact BES Cyber Assets would have LERC (e.g. video surveillance, laptops with wireless cards, and other solutions crossing the asset boundary) and would require electronic access controls. This will be a substantial shift for some entities who were building implementation plans to address LEAP’s at only those sites that had low impact BES Cyber Assets connected via routable connectivity. The new definition would require all sites to have electronic access controls. At minimum, “routable protocol communication” should be changed to “routable protocol connectivity to a BES Cyber System that crosses a BES asset boundary.”	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports comments submitted by Edison Electric Institute. Also, while PacifiCorp understands the justification provided for the approach the SDT took, PacifiCorp believes that the approach adds an increased compliance burden without added benefit to the security of BES, or any assurance that entities will not be asked for a list of BES Cyber Assets at Low Impact BES Assets.	
Likes 0	
Dislikes 0	
Response	
Yvonne McMackin - Public Utility District No. 2 of Grant County, Washington - 4	
Answer	No
Document Name	
Comment	
See commentary submitted by Michiko Sell, Public Utility District No. 2 of Grant County, WA.	
Likes 0	
Dislikes 0	
Response	

ALAN ADAMSON - New York State Reliability Council - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

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

Likes 0	
Dislikes 0	
Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	Yes
Document Name	
Comment	
Good change that supports alignment with R1 part 1.3 and attachment 1, section 3, Low Impact Rating; bi-directional was removed; unidirectional communication promoted the removal; now a data diode is looked at as a control; focus on controls not on if you have a LERC;	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 1, 5, 3; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
This change is good as "Connectivity" is describing what is commonly understood as a physical layer relationship between devices where as "Communication" does not necessarily assume a direct physical layer relationship, as it can be purely logical. This clarification will help entities better develop points of “communications demarcation” as recommended in other impact categories. Understanding those demarcations will give entities the ability to better monitor changes in subject environments that may result in compliance impacts.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Burns & McDonnell - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

Burns & McDonnel believes the proposed modifications meet the intent of FERC's instructions from Order 822 and provide Registered Entities (Entity) sufficient flexibility in determining what is LERC. Our only concern is the proposed definition and associated example diagrams continue to allow BES Cyber Systems (BCS) to be on the same logical network segment as non-BCS Cyber Assets, which allows for the potential use of those non-BCS Cyber Assets to become an attack vector (i.e. pivot point) to the BCS Cyber Assets. While outside of FERC's instructions in Order 822, we feel the standard should address the possibility of a pivot attack much like what is has been implemented for High and Medium Impact BCS and the identification of Protected Cyber Assets (PCA) on the same logical network.

Likes 0	
Dislikes 0	

Response

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy

Answer	Yes
Document Name	

Comment

Occidental Chemical Corporation (OCC) agrees that the concept of direct and indirect access to Low-Impact BES Cyber Systems unnecessarily complicates the assessment of their cyber protections. This differentiation seems to have arisen in CIP v3 in order to develop requirements specific to firewall-protected communications (direct) and remote access communications (indirect). The concept has carried over into CIP v6 – and while it may be appropriate to delve into the details of security controls related to High and Medium-Impact BES assets, it is not the case for Low-Impact facilities.

Likes 0	
Dislikes 0	

Response

Mary Cooper - Alameda Municipal Power - 3,4 - WECC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - NA - Not Applicable - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	
Document Name	
Comment	
signing on with NIPSCO comments of Sarah Gasienica	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF	
Answer	
Document Name	
Comment	

WEC Energy Group (including Wisconsin Electric and Wiscsonsin Publice Service).participated in the development of and support EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Julie Ross - Austin Energy - 3	
Answer	
Document Name	
Comment	
I support Andrew Gallo's comments.	
Likes 0	
Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	
Document Name	
Comment	
We support the comments of TransÉnergie.	
Likes 0	
Dislikes 0	
Response	

2. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 2 Physical Security Controls to reflect the retirement of LEAP. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports comments submitted by Edison Electric Institute. Also, while PacifiCorp understands the justification provided for the approach the SDT took, PacifiCorp believes that the approach adds an increased compliance burden without added benefit to the security of BES, or any assurance that entities will not be asked for a list of BES Cyber Assets at Low Impact BES Assets.	
Likes 0	
Dislikes 0	
Response	

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	
No, unless the proposed LERC definition removing the LEAP term is revised.	
Likes 0	
Dislikes 0	
Response	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Without a LEAP, it is now conceivable that there will be all manner of essentially low to no security access points coming into these low discrete BES assets. That along with the noted communications exemption seems to provide for greater attack surfaces. More discretion on the part of entities in terms of security implementations (cost minimization and cultural inertia), will have the net effect of having less security than if LEAP had been retained. From an attacker's standpoint, why would they go after more secure medium substations when there is an abundance of less secure low substations which can net a comparable effect?	

In BPA's view, the retirement of LEAP and expansion of LERC will increase the number of assets included in the ESP. For example, if you have a substation with multiple buildings but (under the existing version of the standard) only one building has LEAP, you must now secure all buildings. This change will have a negative impact on security levels and actually works against Order 822.

BPA proposes that the SDT retain LEAP and address the Commission's instruction to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition.

Likes 0	
Dislikes 0	

Response

Maggy Powell - Exelon - 6

Answer	No
Document Name	

Comment

See Exelon TO Response

Likes 0	
Dislikes 0	

Response

Ruth Miller - Exelon - 5

Answer	No
Document Name	

Comment

See Exelon TO Response

Likes 0	
Dislikes 0	

Response

John Bee - Exelon - 3

Answer	No
Document Name	

Comment

See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Johnny Anderson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
It appears the SDT is moving away from physically protecting a LEAP associated with LERC but now requires physical protection around devices that provide electronic controls and shouldn't section 2 apply only when LERC exists? The intent on whether to protect a "LEAP" that is no longer defined as a LEAP is unclear.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	

NRECA does not object to the retirement of the term LEAP. However, NRECA suggests modifications to Attachment 1, Section 2 that do not require demonstration of compliance with an air-gap and do not require identification of LERC that is not related to BES facilities. NRECA believes that a solution to this concern could be by revising Attachment 1 Section 2 to add the bold/underlined language: “Cyber asset(s), as specified by the Responsible Entity**, if any,** that provide electronic access control(s) implemented for section 3.1.”

Likes 0	
Dislikes 0	

Response

Tim Kucey - PSEG - PSEG Fossil LLC - 5

Answer	No
Document Name	

Comment

PSEG supports EEI comments

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	No
Document Name	

Comment

We do not agree with these proposed revisions.

We believe the proposed revisions only state “The asset” and not “BES assets.” We ask the SDT if there is a difference. If not, we then request the SDT cease using this term in its presentations.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	No
Document Name	
Comment	

: Exelon supports the retirement of the LEAP definition. Exelon identified one concern with the proposed revisions in Attachment 1 Section 2. The language does not make sense for circumstances where air-gapping is used to provide the electronic access control for LERC as permitted by LERC Reference Model 1 -- Physical Isolation. In those circumstances there is no "Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1." Therefore, it is unclear how a Responsible Entity using air-gapping could comply with Section 2 of Attachment 1. To resolve this issue, Section 2 of Attachment 1 should be revised to add the following qualifier: "Cyber Asset(s), as specified by the Responsible Entity, **if any**, that provide electronic access control(s) implemented for Section 3.1." This change would be consistent with the language in Attachment 2 section 2(b) providing the corresponding Measure.

Likes 0	
Dislikes 0	
Response	

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	
Comment	

FMPA supports the comments of American Public Power Association.

Likes 0	
Dislikes 0	
Response	

Nathan Mitchell - American Public Power Association - 3,4

Answer	No
Document Name	
Comment	

The SDT did not address shared facilities, which is a real concern. Entities should be encouraged to work together to protect BES Cyber Assets, not have to individually protect them “as specified by the Responsible Entity”. In some regions, having multiple owners of asset Facilities, systems, and equipment is very common. This sharing of a single asset becomes even more common in low impact assets. When controlling physical access at the

perimeter of the BES asset, the current language continues to require JRO, CFR, or MOUs. The language should be revised to provide clear guidance in the either attachment 1 or the Guidelines and Technical basis.

The wording of Section 2 suggests that Responsible Entities have to create a list of Cyber Assets, when it is mean to apply only to the Cyber Assets that provide electronic access control for LIBCS.

We recommend moving “as specified by the Responsible Entity” after “that provide electronic access control(s)” to make this intent more clear, i.e., reword as:

“and (2) the Cyber Asset(s) that provide electronic access control(s), as specified by the Responsible Entity, implemented for Section 3.1, if any.”

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Southern Company is a member of the Edison Electric Institute (“EEI”) and generally supports EEI’s comments that are being submitted in response to the proposed modifications.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy supports the comments submitted by Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	No
Document Name	
Comment	

The alternate proposal for Section 2 retains an obligation to protect the Cyber Asset(s) interface (reference FERC-approved LEAP definition) and provides flexibility to protect Cyber Asset(s) providing electronic access control(s), for example, if interface is not the concept of the control. This is important to carry over the in-progress V6 implementation into V7.

Alternate proposal: after “(2) the Cyber Asset(s)” insert “or Cyber Asset(s) interface,” As a result of the alternate proposal for question 3, change the reference from “Section 3.1” to “Section 3.” So it reads as: “Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s) or Cyber Asset(s) interface, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3, if any.”

Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry
Dislikes 0	

Response

Christy Koncz - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG	
Answer	No
Document Name	
Comment	

PSEG agrees with and supports EEI's comments.

Likes 1	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

The wording of Section 2 suggests that Responsible Entities have to create a list of Cyber Assets, when it is mean to apply only to the Cyber Assets that provide electronic access control for LIBCS.

We recommend moving “as specified by the Responsible Entity” after “that provide electronic access control(s)” to make this intent more clear, i.e., reword as:

“and (2) the Cyber Asset(s) that provide electronic access control(s), as specified by the Responsible Entity, implemented for Section 3.1, if any.”

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

This response depends on the approach ultimately developed by the SDT to address the FERC directive outlined above. Texas RE would note at this time that LEAPs represent a familiar and understood concept, so substituting access point demarcations for other concepts may introduce additional confusion into the Reliability Standards.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CIP-003-7, Attachment 1, Section 2b, as written suggests that the Responsible Entity is required to have a list of Cyber Assets. CenterPoint Energy believes the intent of the requirement is to control physical access to Cyber Assets used to provide electronic access control for low impact BCS.

CenterPoint Energy recommends the following edits:

“(2) the Cyber Asset(s) that provide electronic access control(s) implemented for Section 3.1, as specified by the Responsible Entity, if any.”

Likes 0	
Dislikes 0	

Response

Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	No
Document Name	
Comment	
SCE agrees with and supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
See question 1 comment.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	No
Document Name	
Comment	
ITC Holdings disagrees with the retirement of the term LEAP. The term LEAP allows you to delineate which device is performing the electronic access control. By retiring this term it will leave each entity to make up their own term for the device that will perform the electronic access control.	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No

Document Name	
Comment	
While the defined term LEAP simplified Cyber Asset categorization, it is not absolutely necessary. In some regions, such as FRCC, having multiple owners of asset Facilities, systems, and equipment is very common. This sharing of a single asset becomes even more common in low impact assets. When controlling physical access at the perimeter of the BES asset, the current language continues to require JRO, CFR, or MOUs. The language should be revised to provide clear guidance in either attachment 1 or the Guidelines and Technical basis.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Based on our understanding of the new definition of LERC and the retirement of LEAP, OCC expects to use a defense-in-depth approach to provide physical protection for our Low-Impact facilities and our Low-Impact BES Cyber Systems. In our view, the new language in the Physical Security Controls section of Attachment 1 and the guidance section allow for this approach. Although we understand that the drafting team does not govern compliance, OCC would be concerned if our reading of the intent of the modifications is not accurate. If it is, then other Registered Entities and Compliance Enforcement Authorities will be confused as well – leading to inconsistent application of the requirements.	
Likes 0	
Dislikes 0	
Response	
Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker	
Answer	Yes
Document Name	
Comment	
Please also see the comments submitted by the National Rural Electric Cooperative Association (NRECA).	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	

Answer	Yes
Document Name	
Comment	
N&ST agrees with the update to CIP-003-6, Attachment 1, Section 2 Physical Security Controls.	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
AZPS is in agreement with the retirement of LEAP.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Burns & McDonnell - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	

Comment	
Although Austin Energy (AE) agrees with removing the term "LEAP," we believe the SDT should define the term “electronic access control” to remove ambiguity from the proposed Standard. In the Guidelines document, the SDT provides examples of electronic access controls (restricting IP addresses, ports, or services; authenticating users; air-gapping networks; terminating routable protocol sessions on a non-BES Cyber Asset; implementing unidirectional gateways). We recommend the SDT define the term “electronic access controls” (and provide the examples as part of the definition).	
Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	
Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	Yes
Document Name	
Comment	
Basically added access control devices to the list to physically protect? No LEAPs now but access controls need physical security;	
Likes 0	
Dislikes 0	
Response	
Yvonne McMackin - Public Utility District No. 2 of Grant County, Washington - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Bradley Collard - SunPower - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michiko Sell - Public Utility District No. 2 of Grant County, Washington - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Oshani Pathirane - Oshani Pathirane On Behalf of: Paul Malozewski, Hydro One Networks, Inc., 1, 3; - Oshani Pathirane	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Barnett - Exxon Mobil - 7	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - NA - Not Applicable - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no NextEra	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey Watkins - Jeffrey Watkins On Behalf of: Eric Schwarzrock, Berkshire Hathaway - NV Energy, 5; - Jeffrey Watkins	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Oliver Burke - Entergy - Entergy Services, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
ALAN ADAMSON - New York State Reliability Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Tallman - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name LG&E and KU Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Emily Rousseau - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO-NERC Standards Review Forum (NSRF)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 1, 5, 3; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Varnell - Tenaska, Inc. - Tenaska Power Services Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mary Cooper - Alameda Municipal Power - 3,4 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	
Document Name	
Comment	
We support the comments of TransÉnergie.	
Likes 0	
Dislikes 0	
Response	
Julie Ross - Austin Energy - 3	
Answer	
Document Name	
Comment	
I support Andrew Gallo's comments.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF	
Answer	
Document Name	
Comment	
WEC Energy Group (including Wisconsin Electric and Wiscsonsin Publice Service).participated in the development of and support EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	

Answer	
Document Name	
Comment	
signing on with NIPSCO comments of Sarah Gasienica	
Likes 0	
Dislikes 0	
Response	

3. Requirement R2: The SDT revised CIP-003-6, Attachment 1, Section 3 Electronic Access Controls to require entities to implement electronic access control(s) for LERC, if any, to permit only necessary electronic access to low impact BES Cyber System(s). Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

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

Answer	No
Document Name	

Comment

LERC Reference Model 7 – User Authentication includes a sentence that states “The electronic access control depicted in this reference model may not meet the security objective for controlling device-to-device communication across the LERCdepending on the specific system configuration in place.”. Clarify the sentence by including a specific example that would be compliant versus one that would be non-compliant.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5

Answer	No
Document Name	

Comment

The proposed definition raises more ambiguity than the current definition and goes beyond the direction of the FERC order.

Likes 0	
Dislikes 0	

Response

Emily Rousseau - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO-NERC Standards Review Forum (NSRF)

Answer	No
Document Name	Project 2016-02 sonet.JPG

Comment

It is unclear how to document LERC electronic access controls, especially for physically isolated and logically isolated systems. Do we need to have detailed network drawings? Do we need to label devices and ports for identification during an audit? Can the documentation be a list? Does the list have to identify each LERC individually or just list the electronic access control types implemented at each asset? How is the documentation for larger networks expected to be validated?

Likes 0	
Dislikes 0	

Response

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

The proposed revision is not adequately defined or effectively auditable. The expectation defined in the Guidelines and Technical Basis under Determining LERC does not provide adequate definition of the asset boundary. As such, it is unclear what the asset boundary is. Under this guideline, the asset could be defined as the Facilities, systems, and equipment (a set of hardware and Cyber Assets) that is used within the asset, the Cyber Assets that make up the asset, the physical security border of the asset, or the electronic security border of the asset. Depending on the choice made, the results would be very different with respect to what is crossing the boundary and whether serial to IP converters are included. This lack of definition will result in another round of unclear interpretation of the standard. We have seen where this lack of clear definition led us over the past three years in the Lessons Learned program.

If the intent is for the entity to have full flexibility to define the boundary, there is no clear guidance in the standard that this is allowed. There is tremendous flexibility for both entities and auditors. Clear guidance should be provided prior to approving the Standard, especially for low impact generation locations.

Further, would it be appropriate to address additional concerns identified in the FERC NOI by adding a requirement that any LERC that passes information to any high or medium impact ESP utilizing a transmission path that is not exclusively dedicated to communications for use by an Entity or between Entities is not permitted (or at least must be identified so that the risk is recognized)?

Likes 0	
Dislikes 0	

Response

Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns

Answer	No
Document Name	

Comment

Comments: We would suggest to the drafting team that some alternative language should be used in reference to the phrase ‘only necessary’ in Section 3. Suggested alternative language as followed:

‘ to permit only necessary as determined by Responsible Entity’ pertaining to Electronic Access Controls’.

Likes 0	

Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

See question 1 comment.

Likes 0	
Dislikes 0	

Response

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer	No
Document Name	

Comment

The revised requirement, and accompanying discussion the CIP-003-7 Supplemental Material, is unnecessarily unclear as regards inbound and outbound access for Low impact BES Cyber Systems having LERC, and in this specific regard does not represent an improvement on the existing requriement. To avoid unnecessary confusion, please revise requirement to clarify.

- If both inbound and outbound access are in scope, revise requirement to state so, such as “Implement electronic access control(s) for LERC, if any, to permit only necessary INBOUND AND OUTBOUND electronic access to low impact BES Cyber System(s).”
- If only inbound access is in scope, revise requirement to state “Implement electronic access control(s) for LERC, if any, to permit only necessary INBOUND electronic access to low impact BES Cyber System(s)” (CAPITALS indicate additions).

The “Determining Access Controls” discussion in the CIP-003-7 Supplemental Material similarly should be revised to clearly state whether the term ‘access’ applies to inbound and outbound access or only to inbound access.

Please also indicate if a single electronic access control is sufficient for all sources of LERC existing at an asset (site) or if individual sources of LERC must be individually identified and appropriate controls implemented for each (this point and related matters are further discussed below in comments for Question 4, Measure M2).

Likes 0	
Dislikes 0	

Response

Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	No
Document Name	
Comment	
SCE agrees with and supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Robert Tallman - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name LG&E and KU Energy	
Answer	No
Document Name	
Comment	
LG&E/KU supports EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
The proposed revisions to the Low Impact External Routable Connectivity (LERC) definition, retirement of the Low Impact Electronic Access Point (LEAP) and associated changes to the requirements for CIP-003 Attachment 1 Section 2 and 3 represent a significant shift from the currently FERC-approved definitions and requirements. The proposed changes include identifying LERC to non-BES Cyber Assets increasing the scope. Entities are well into their implementation of the approved definitions and requirements. This fundamental shift creates regulatory uncertainty for entities and timing concerns to meet the proposed implementation schedule due to re-work and the volume of assets containing low impact BES Cyber Systems. At best, FERC approval is not likely till near the end of 2017, which will be too late for most entities’ budgeting schedules for work to be completed in 2018 if the revised requirements require budget changes. It’s not logical to vote yes on the non-binding poll until the requirement language is closer.	
Likes 0	
Dislikes 0	
Response	

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
The way it is worded does not provide any security benefit. For instance, reference model number 5 is an example that is not represented by the verbiage. We propose, “Implement electronic access control(s) to permit only necessary electronic communications to Low Impact BES Cyber System(s) at assets in which LERC exists.”	
Likes 0	
Dislikes 0	
Response	

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy believes that the registered entities are in the best position to determine the necessary electronic access controls for their specific environment because they own and/or operate the systems. CenterPoint Energy recommends the following edits to CIP-003 Attachment 1, Section 3.1: **“Implement electronic access control(s) for LERC, if any, to permit only necessary electronic access to low impact BES Cyber Systems, as determined by the Responsible Entity.”**	
Likes 0	
Dislikes 0	
Response	

Julie Hall - Entergy - 6	
Answer	No
Document Name	
Comment	
The Supplemental Material qualifies LERC as “an attribute of a BES Asset… without regard to connectivity to Cyber Assets within the BES Asset” and further states that “LERC can exist for a BES Asset even if there is no routable protocol connectivity to any Low Impact BES Cyber System within the BES Asset.” With the statement that LERC can exist without a connection to a Low Impact BES Cyber System, and Attachment 1 Section 3 Part 3.1 requiring the implementation of “electronic access control(s) for LERC, if any”, the risk of an inadvertent increase in scope referenced in the comments in Question #1 above is again evident with this change as controls would be implemented to secure LERC even though there is no LERC *connection* to a Low Impact BES Cyber System. Therefore, Cyber Assets that would normally be considered out-of-scope could inadvertently be included in this	

case. CIP-003-7 R2 requires the implementation of “cyber security plan(s) for its low impact BES Cyber Systems”, and illustrates the anticipated scope of the requirement as being the protection of Low Impact BES Cyber Systems, not LERC. It is requested that additional clarification be added to Attachment 1 Section 3 Part 3.1 to specify that controls must be implemented to protect Low Impact BES Cyber Systems that *participate* in LERC, not for *any instance* of LERC.

Likes 0	
Dislikes 0	

Response

Oliver Burke - Entergy - Entergy Services, Inc. - 1

Answer	No
Document Name	

Comment

I support comments submitted by Entergy's Julie Hall.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE suggests an asset list and/or diagrams is the best way to identify its low impact BES Cyber Systems and possibly confirm electronic access control applied.

Attachment 1 Section 3 potentially conflicts with the note in Requirement R2 since it *does* ask for a diagram or list of implemented electronic access controls.

Texas RE is concerned the actions Section 3 asks entities does not give the full picture. Even though the diagrams would show electronic access control implemented, it would not show the low impact BES Cyber Systems the electronic access control was implemented on.

Likes 0	
Dislikes 0	

Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

In addition to addressing the concerns we mentioned in our answer to question 1, Section 3 should clarify that Responsible Entities should determine whether the electronic access is necessary as they are in the best position to make those determinations because they own and/or operate these systems.

To address these issues, as well as our question 1 and 6 issues, EEI makes an alternative text recommendation for Section 3 below. We encourage the SDT to clearly state the security objective and allow entities to decide how best to provide evidence in the light of the circumstances at their particular assets.

"Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access, based on need as determined by the Responsible Entity, to the low impact BES Cyber Systems that use (1) a routable protocol leaving or entering the asset containing the low impact BES Cyber Systems, if any, and (2) Dial -up Connectivity, if any. This excludes communications between intelligent electronic devices used for time -sen protection or control functions between non-Control Center BES assets containing low impact BES Cyber Systems including, but not limited to, IEC 61850 GOOSE or vendor proprietary protocols.

For routable connectivity, electronic access may be controlled using one or more of the following security controls:

- Physical isolation of the low impact BES Cyber System(s) from the external routable protocol, communication, i.e., an air gap
- A uni-directional gateway
- Logical isolation of the low impact BES Cyber System(s) from the external routable protocol communication, which may include an isolated network segment with logical controls, a host-based firewall, network-based access controls, a Cyber Asset that requires authentication and then establishes a new connection to the low impact BES Cyber System, or other method of logical isolation
- A layer 7 application layer break or other protocol break
- Some other electronic access control that does not allow unauthorized access to the low impact BES Cyber Systems from an external user or device

For Dial-up Connectivity, electronic access may be controlled using one or more of the following security controls:

- Dial-back modems
- Modems that must be remotely enabled or powered up
- Modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use
- Some other electronic access control that does not allow unauthorized dial-up access to the low impact BES Cyber Systems from an external user or device"

EEI also raises a concern our members have with regards to the use of "non-Control Center BES" in the current LERC definition and the above alternative language we proposed. We understand that the SDT was trying to address a technical challenge specific to relay tripping schemes that have millisecond time-sensitivities and was trying exclude normal "poll every few seconds" SCADA traffic as "time-sensitive." We agree that a SCADA system that needs to poll every 2-3 seconds should be protected as firewalls can easily accommodate these requirements. However, there may be scenarios where a Remedial Action Scheme could have components (possibly even the controller itself) in a low impact control center that requires sub-second communication capability, which are not compatible with existing electronic access controls. We recommend that the SDT consider this technical challenge to avoid unintended consequences to reliability and/or compliance.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Response

Jeffrey Watkins - Jeffrey Watkins On Behalf of: Eric Schwarzrock, Berkshire Hathaway - NV Energy, 5; - Jeffrey Watkins

Answer	No
Document Name	

Comment

It is unclear how to document LERC electronic access controls, especially for physically isolated and logically isolated systems. Do we need to have detailed network drawings? Do we need to label devices and ports for identification during an audit? Can the documentation be a list? Does the list have to identify each LERC individually or just list the electronic access control types implemented at each asset? How is the documentation for larger networks expected to be validated?

Likes 0	
Dislikes 0	

Response

Christy Koncz - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG

Answer	No
Document Name	

Comment

PSEG agrees with and supports EEI's comments.

Likes 1	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

Suggested wording for Attachment 1 Section 3.1: “Implement technical and/or procedural controls to permit only necessary electronic communications to low impact BES Cyber Systems and to mitigate the risk of unauthorized electronic access to BES Cyber Systems.” Please consider eliminating the

definition of LERC and eliminating reference to LERC in Attachment 1 Section 3. The definition of LERC is too broad, will cause confusion regarding the concept of asset “boundary” and permits risk due to the exclusion of “time-sensitive” communications.

We support the SDT approach of not prescribing how Responsible Entities meet the security objective. The non-exclusive examples described in the Measure and Guidelines are useful.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

It isn’t clear how to document LERC electronic access controls, especially for physically isolated and logically isolated systems. We would be opposed to having to provide detailed network drawings for all Low Impact assets. If a list would suffice then would it require identification of each LERC individually or simply the electonric access control types. How will this information be validated. Lets not forget that these are by definition LOW IMPACT.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

It isn’t clear how to document LERC electronic access controls, especially for physically isolated and logically isolated systems. We would be opposed to having to provide detailed network drawings for all Low Impact assets. If a list would suffice then would it require identification of each LERC individually or simply the electonric access control types. How will this information be validated. Lets not forget that these are by definition LOW IMPACT.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO

Answer	No
Document Name	
Comment	

This represents a significant change from the previous version creating regulatory uncertainty and possible re-work of already completed work for hundreds to thousands of assets depending on the size of the Entity. Entities have already started to implement based on the currently approved version. This level of change creates timing issues and concerns for meeting the proposed implementation schedule. The alternate proposal adds clarity on a layer 7 application layer break using language from the Guidelines and Technical Basis, which was referenced by FERC in Order 822. The alternate proposal also (1) reflects removal of LERC and LEAP definition, (2) keeps the FERC-approved obligations to protect routable and Dial-up Connectivity, (3) removes “user-initiated interactive”, “device-to-device: and “direct” references, (4) retains the concept of “bidirectional” from the FERC-approved LERC definition by using “leaving or entering”, (5) moves time-sensitive protection and control functions exclusion from LERC definition to Att. 1 Section 3 and expands it to include comparable time-sensitive protection and control functions for generation and for possible sub-second communications between a Remedial Action Scheme and a low impact Control Center. (Perhaps time-sensitive or words to that effect needs to be defined.)

Alternate proposal: Each Responsible Entity shall control electronic access, based on need as determined by the Responsible Entity, to low impact BES Cyber Systems that use: (1) a routable protocol leaving or entering the asset containing the low impact BES Cyber Systems, if any, and (Dial-up Connectivity, if any. This excludes communications: (1) between intelligent electronic devices used for time-sensitive protection or control functions between BES assets containing low impact BES Cyber Systems including, but not limited to, IEC 61850 GOOSE or vendor proprietary protocols; (2) when there is a layer 7 application layer break or a Cyber Asset requires authentication and then establishes a new connection to the low impact BES Cyber System (A complete security break does not allow access to the low impact BES Cyber Systems from an external user or device); or (3) when there is no bidirectional routable or Dial-up Connectivity to low impact BES Cyber Systems at the asset.

Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	
Comment	

Duke Energy supports the comments submitted by Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment
Southern Company is a member of the Edison Electric Institute (“EEI”) and generally supports EEI’s comments that are being submitted in response to the proposed modifications.

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4

Answer	No
Document Name	

Comment
The revisions are not clear. While we agree that only necessary electronic access should be allowed, the definition of ‘asset boundary’ keeps the requirement from being implemented in a straightforward way. It is also uncertain how this guideline will be applied during an audit. The term asset is undefined and there are no provisions for prescribing what that might include. This makes the definition lack clarity and makes it more difficult for entities to determine and protect LERC if it might exist.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment
We would suggest to the drafting team that some alternative language should be used in reference to the phrase ‘only necessary’ in Section 3. Suggested alternative language as followed: ‘ to permit only necessary as determined by Responsible Entity’ pertaining to Electronic Access Controls’.

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	

Comment

FMPA supports the comments of American Public Power Association.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST believes the revised requirement statement for electronic access controls (Attachment 1, Section 3) to "permit only necessary electronic access to low impact BES Cyber System(s)" is vague and therefore could be subject to a wide variety of interpretations. Concerns include:

- The phrase, "access *to*" low impact BES Cyber System(s) could be interpreted to mean that only inbound connections to BES Cyber Systems must be controlled. N&ST assumes this is not the SDT's intent, based on the fact several revised "LERC Reference Models" in the CIP -003- 7 D Supplemental Material section describe the use of "inbound and outbound" access controls. N&ST recommends that the Attachment 1 Section 3 requirement for electronic access control retain the existing "inbound and outbound" language so as to avoid controversy over the Standard's intent.

- The revised "examples of evidence" for electronic access controls (Attachment 2, Section 3) lists "authenticating users" as one approach. If an entity authenticates users who are accessing low impact BES Cyber Systems, has the electronic access control requirement been fully addressed? N&ST believes the answer is or should be "No," as authenticating users may not, by itself, fully control inbound access and does not control outbound access at all. LERC Reference Model 7 ("User Authentication") makes note of this very problem with the comment, "The electronic access control depicted in this reference model may not meet the security objective for controlling device -t system configuration in place." N&ST recommends that the requirement statement in Attachment 1 make it explicit that electronic access controls must be applied to both user-to-device and device-to-device communications where LERC exists and one or both of the communicating devices is a low impact BES Cyber System. N&ST also recommends that the "examples of evidence" section for electronic access controls be revised to make it clear that in cases where there are both user-to-device and device-to-device communications via LERC, a combination of controls may be required.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1	
Answer	No
Document Name	
Comment	

Comment 1: The currently proposed language could be read to require electronic access controls for both BES and non-BES Cyber Assets. While Exelon does not think that is the intent of the language, the intent should be clearer. In addition, the order of the assessment and application of the electronic access controls could be better understood with a subtle change in the sequence of the requirement language. Please consider the following revision: "For asset(s) containing low impact BES Cyber System(s) with LERC, if any, implement electronic access controls to permit only necessary electronic access to the low impact BES Cyber System(s)."

Comment 2: Also, continuing the discussion from the response to Q1, Exelon presents the following proposals for SDT consideration in addressing the concerns raised.

Proposal Q3A – Using the LERC definition proposed in Q1 (Q1A –simply remove 'direct'), the following requirement proposal removes the obligation to inventory and maintain evidence of every routable connection at the asset containing the low impact BES Cyber System as well as having to define and support what the Responsible Entity determines is the "asset boundary" for identifying routable connections. Instead this proposal focuses the obligation on the performance of the security objective associated with electronic access controls for the asset containing low impact BES Cyber Systems.

SECTION 3. Electronic Access Controls: Each Responsible Entity shall:

3.1 For asset(s) containing low impact BES Cyber System(s) with LERC, if any, implement one or more of the following method(s) to achieve the objective of applying electronic access control(s) to permit only necessary electronic access to low impact BES Cyber Systems:

- Physical isolation
- Logical isolation
- Host-based inbound and outbound access permissions
- Network-based inbound and outbound access permissions
- Centralized network-based inbound and outbound access permissions
- Uni-directional gateway
- Jump host located within the asset containing the low impact BES Cyber System
- Session termination within the asset containing the low impact BES Cyber System
- Other method(s) to achieve the objective of applying electronic access control(s) for LERC

3.2 Implement authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability.

Additionally, to support this proposal, LERC Reference Model 7 – User Authentication should be updated to focus on the use of a "jump host" which would meet the security objective of electronic access controls for LERC instead of how the model is written which does not itself necessarily achieve the security objective as stated in the text of the model.

Proposal Q3.2: Alternatively, the following is another proposal that meets the FERC directive to address "direct," aligns the compliance language to the approach used for Section 2 of Attachment 1 for Physical Security and incorporates the concepts from the LERC definition into the obligation language; thereby removing the need for the separate definition. This proposal retains the examples from the GTB that provide electronic access controls.

SECTION 3. Electronic Access Controls: Each Responsible Entity shall control electronic access, based on need as determined by the Responsible Entity, to low impact BES Cyber Systems that use (1) a routable protocol leaving or entering the asset containing the low impact BES Cyber System(s), if any, and (2) Implement authentication for all Dial ity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Communications between intelligent electronic devices used for time able protocol between non Center BES assets containing low impact BES Cyber Systems is excluded from Section 3; including, but not limited to, IEC 61850 GOOSE or vendor proprietary protocols.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb

Answer	No
Document Name	

Comment

Concern—Creates Onerous Compliance Tasks: We would reiterate, as detailed in our Question No. 1 comments under the subheading, Security for Security's Sake. When the scenario is considered that would, for all intents and purposes, bring every substation into the scope of applicability and then require Electronic Access Controls (EAC) for each substation, the task to install and maintain firewalls and their associated rules under CIP-005-5 would tax most, if not all Entities, to comply.

We recognize there are offered alternatives but regardless of the EAC, it is a substantial, arduous, and resource consuming activity with a likely limited benefit to BES Reliability.

Again, the scenario and its likely impact highlights, there is a reason they call them "low impact" assets. We question whether requiring firewalls or other Electronic Access Controls at every substation materially improves BES reliability and security.

Proposal

As previously offered, a modification to the proposed LERC term would temper the potential scope of applicability to only routable protocols connected to low impact BES Cyber Systems.

“A routable protocol communication that crosses the boundary of an asset connected to one or more low impact BES Cyber Systems…”	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
We do not agree with these proposed revisions. FERC has a Notice of Inquiry, Docket No. RM15-14-002 and RM16-18-000, that is asking whether air-gapping networks are sufficient for network security. We believe the minimum level of Electronic Access Controls available is insufficient to address these inquiries.	
Likes 0	
Dislikes 0	
Response	
Tim Kucey - PSEG - PSEG Fossil LLC - 5	
Answer	No
Document Name	
Comment	
PSEG supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	

NRECA believes the proposed language could be understood to require electronic access controls for BES and non-BES Cyber Assets. The proposed language should be revised to clarify that the scope does not apply to non-BES Cyber Assets. This can be accomplished by specifically addressing only “low impact BES Cyber Systems” in the language in order to remove the ambiguity regarding non-BES Cyber Assets.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3

Answer	No
Document Name	

Comment

Cowlitz PUD supports the comments supplied by APPA.

Likes 0	
Dislikes 0	

Response

Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker

Answer	No
Document Name	

Comment

In general, we do not support the air gap as an electronic access control mechanism. Demonstration of an "air gap" is a requirement to validate in the negative. In effect, Responsible Entities must provide proof of a connection that was never initiated. For example, the use of a smartphone introduces routable communications that crosses the asset boundary creating LERC. Using the air gap concept, the Responsible Entity must now account for that connection and be able to demonstrate that an air gap exists between it and the low impact BES Cyber Assets. This is overly burdensome. As a result, we propose that the air-gapping concept be excluded from scope.

Likes 0	
Dislikes 0	

Response

John Bee - Exelon - 3

Answer	No
Document Name	

Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Ruth Miller - Exelon - 5	
Answer	No
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Exelon - 6	
Answer	No
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

The proposed change in language expands the scope but does not reduce the ambiguity as required by 822. There is not a prescribed, measurable process for how an entity can “permit only necessary electronic access to low impact BES Cyber System(s)” and prove compliance without a complete inventory within the asset boundary. BPA believes this means that every asset within a Low BES can conceivably have its own access control of varying sophistication. This will, like Question 2, encourage the least costly compliance-driven controls be put forth as meeting an interpretation of the regulation. The result will be widely varying practice and commensurate security levels. BPA believes this changes the focus from device level language to asset level and vastly increases the number of devices that will be subject to compliance. Again, the decision to do away with a LEAP has a cascade effect in what will likely result in creating less security as multiple devices will be directly reachable via routable communications and each will have to have its own security.

Likes 0	
Dislikes 0	

Response

Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

The revised requirement, and accompanying discussion the CIP-003-7 Supplemental Material, is unnecessarily unclear as regards inbound and outbound access for Low impact BES Cyber Systems having LERC, and in this specific regard does not represent an improvement on the existing requriement. To avoid unnecessary confusion, please revise requirement to clarify. If both inbound and outbound access are in scope, revise requirement to state so, such as “Implement electronic access control(s) for LERC, if any, to permit only necessary INBOUND AND OUTBOUND electronic access to low impact BES Cyber System(s).” If only inbound access is in scope, revise requirement to state “Implement electronic access control(s) for LERC, if any, to permit only necessary INBOUND electronic access to low impact BES Cyber System(s)” (CAPITALS indicate additions).

The “Determining Access Controls” discussion in the CIP-003-7 Supplemental Material similarly should be revised to clearly state whether the term ‘access’ applies to inbound and outbound access or only to inbound access.

Likes 0	
Dislikes 0	

Response

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray

Answer	No
Document Name	

Comment

Based on the proposed definition of LERC, all substations containing Low Impact BES Cyber Assets will have LERC. In this case, and due to the removal of routable protocol access statements, it is unclear what electronic access is required (e.g. remote electronic access versus a Technician directly connecting to a BES Cyber Asset via a serial interface while standing in front of the BES Cyber Asset).

Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	

Answer	Yes
Document Name	
Comment	
Adds EACMS as a required for Low Impact when external rroutable connectivity or Dial Up exists; what does the flexibility look like mentioned on page 30?	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
We believe the SDT should define “electronic access control” to remove ambiguity from the proposed Standard. In the Guidelines document, the SDT provides examples of electronic access controls (restricting IP addresses, ports, or services; authenticating users; air-gapping networks; terminating routable protocol sessions on a non-BES Cyber Asset; implementing unidirectional gateways). We recommend the SDT define the term “electronic access controls” (and provide the examples as part of the definition).	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 1, 5, 3; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
This is good because the criteria that results in a device being classified as a “Low Impact” asset is narrowly formed from a "Reliability Impact" perspective and not from a security perspective. The reliability concern is independent of its security risk to other environments. As so, the emphasis on “controlling access” is a step in the right direction to meaningfully achieving security.	
Likes 0	
Dislikes 0	
Response	

Michael Johnson - Burns & McDonnell - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Burns & McDonnell has noticed many comments regarding the “implement electronic access control(s)” language of the proposed requirement is causing some concern with Registered Entities (Entity), with most of those comments related to bring into scope non-BES Cyber Systems (BCS). We feel most of those concerns are valid based on a lack of information within the Guidenace and Technical Basis (GTB) section on what has to be identified and to what extent the identification has to be for non-BCS communications. Burns & McDonnell recommends the Standard Drafting Team (SDT) provide additional clarity in the GTB section on what documentation is required for the non-BCS communcations to help guide Entities in the development of their documentation.	
Likes 0	
Dislikes 0	
Response	

Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
AZPS is in agreement with the revision to require implementation of electronic access controls for LERC to permit only necessary electronic access to low impact BCS; however, respectfully requests that examples of such controls (not all inclusive) be provided in Attachment 1rather than as part of the examples of evidence in Attachment 2. Inclusion of examples such as those listed in Attachment 2 - restricting IP addresses, ports, or services; authenticating users; air-gapping networks; terminating routable protocol sessions; and implementing unidirectional gateways - will ensure that entities employ a secure method to protect LERC, which reduces risk to the BES. Additionally, the Supplemental Material section for Requirement R2, Attachment 1, Section 3 - Electronic Access Controls states that “control(s) must allow only “necessary” access as determined by the Responsible Entity and they need to be able to explain the reasons for the electronic access permitted with their electronic access controls …[which] can be documented within the Responsible Entity’s cyber security plan(s) or other policies or procedures associated with the electronic access controls” (CIP-003-6 Redline, Page 32). AZPS respectfully requests that the Standard Drafting Team Supplemental Materials should not add new or different obligations or expectations to requirements, but, rather, clarify them. AZPS respectfully asserts that the statement requiring reasons for permitted electronic access could be interpreted as adding obligations or expectations that are not included in the actual requirement language. Accordingly, AZPS requests that the SDT remove the reference to documentation of or explanation of reasons for electronic access in cyber security plan(s) from the Supplemental Material section.	
Likes 0	
Dislikes 0	
Response	

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy

Answer	Yes
Document Name	
Comment	

OCC agrees that the identification of the proper boundary for the Low-Impact facility is a much more straight-forward process than attempting to differentiate between direct and indirect access. In our view, this still assures that every communication path that enters or leaves our facility will be properly assessed. We can then determine the most appropriate physical and cyber protections for each, on a case-by-case basis.

OCC is relying heavily on the language in the requirements, measures, and GTB to assure compliance with the requirement. We did not find any gaps in the materials, but would hope that the drafting team captures any new relevant examples that may arise during the review of CIP-003-7.

Likes 0	
Dislikes 0	
Response	

Mary Cooper - Alameda Municipal Power - 3,4 - WECC

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

John Varnell - Tenaska, Inc. - Tenaska Power Services Co. - 6

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
ALAN ADAMSON - New York State Reliability Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no NextEra	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - NA - Not Applicable - SPP RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jay Barnett - Exxon Mobil - 7	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Oshani Pathirane - Oshani Pathirane On Behalf of: Paul Malozewski, Hydro One Networks, Inc., 1, 3; - Oshani Pathirane	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Johnny Anderson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michiko Sell - Public Utility District No. 2 of Grant County, Washington - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Yvonne McMackin - Public Utility District No. 2 of Grant County, Washington - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	
Document Name	
Comment	
signing on with NIPSCO comments of Sarah Gasienica	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF	
Answer	
Document Name	
Comment	
WEC Energy Group (including Wisconsin Electric and Wiscsonsin Publice Service).participated in the development of and support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Julie Ross - Austin Energy - 3	
Answer	
Document Name	
Comment	
I support Andrew Gallo's comments.	
Likes 0	
Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	

Document Name	
Comment	
We support the comments of TransÉnergie.	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	

4. Measure M2: The SDT revised the complementary language of CIP-003-6, Attachment 2, Sections 2 and 3 to make the evidential language of the Measure consistent with the revised requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray

Answer	No
Document Name	

Comment

This is based on the response to Q1. The definition needs to be very clear in its requirements so that the appropriate measures can be applied.

Likes 0	
Dislikes 0	

Response

Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker

Answer	No
Document Name	

Comment

More specifically, our concern is with the wording of Attachment 2 Section 3 Paragraph 1. The comma usage seems to distort the meaning of the paragraph. We recommend the following; "Documentation of implemented electronic access controls (e.g., restricting IP addresses, ports, or services; authenticating users; air gapping, gateway, jump host, directional gateways, etc.) showing that LERC at each asset or group of assets containing low impact BES Cyber Systems is confined only to the access the Responsible Entity deems necessary."

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3

Answer	No
Document Name	

Comment

See Question 3.

Likes 0	

Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
NRECA recommends that the SDT provide specific examples of compliance measures when there is no LERC or dial-up connectivity present.	
Likes 0	
Dislikes 0	
Response	
Tim Kucey - PSEG - PSEG Fossil LLC - 5	
Answer	No
Document Name	
Comment	
PSEG supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	
Concern—Compliance: As detailed in our Question No. 1 comments, the proposed LERC term may convert assets to BES Cyber Assets, bringing CIP-002-5.1 into play and appreciably increase compliance obligations. The proposed language to CIP-003-6, Attachment 2, Sections 2 and 3 reinforces our concern that the proposed LERC term may have the unintended consequence of requiring Entities to create comprehensive BES Facility inventories to evidence compliance under CIP -002- 5.1.	

While such inventories are not explicit in CIP-003-6, Attachment 2, Sections 2 and 3, the plain interpretation suggests evidence is basically requiring an inventory of all low impact BES Cyber Assets and how they were determined.

Proposal

Accept *pro forma* schematics and diagrams representative of categories of LERC BES Cyber Systems. For example, if an Entity's 161kv substations all have a LERC connected to a BES Cyber Asset, that the *pro forma* schematic/diagram is sufficient without a comprehensive list.

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	

Comment

In Section 3, there are no measures/documentation identified for the specific case that LERC or Dial-up does not exist. The applications guideline states "[i]n the case where there is no LERC or Dial [illegible] low impact cyber security plan(s)." Please provide specific examples of compliance measures when there is no LERC or Dial-up Connectivity present.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

Attachment 2 Section 3: Documentation – "termination routable protocol sessions on a non-BES Cyber Asset" is not good. This could lead to a "pivot attack" if the non-BES Cyber Asset it compromised. Also what happens if the connection is routed through the non-BES Cyber Asset and back to a BES-Cyber Asset? This would only make sense if the connection terminated at the non-BES Cyber Asset and that asset could only communicate wth the Low Impact BES Cyber Asset. Additionally, we would recommend adding a common after the close parenthesis (in the first sentence) to help improve the grammar structure of the paragraph. Also, we would suggest to the drafting team to add more clarity on what model 7 and model 8 can be used for and the documentation required to support the process.

Likes 0	

Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company is a member of the Edison Electric Institute (“EEI”) and generally supports EEI’s comments that are being submitted in response to the proposed modifications.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy supports the comments submitted by Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	No
Document Name	
Comment	
The proposed change requires evidence of LERC to non-BES Cyber Assets. Alternate proposal: The alternate proposal (see question 3) would require corresponding changes to Attachment 2 measure for Sections 2 and 3 to make it consistent with the alternate proposal revisions.	
Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry

Dislikes 0	
Response	
Christy Koncz - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG	
Answer	No
Document Name	
Comment	
PSEG agrees with and supports EEI's comments.	
Likes 1	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
In addition to our other concerns, the SDT should make it clear that a device that provides electronic access controls, such as in Reference Models 7 and 8, is not considered a BES Cyber Asset. EEI recommends addressing this by adding the following text to M2: “Note: A Cyber Asset that provides electronic access control(s) under R2 is not a low impact BES Cyber Asset.”	
Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	

To the extent that the models are revised per industry comments including those of the SPP RE, this section will need to be modified. The SPP RE is concerned that the allowance of terminating routable protocol sessions on a non-BES Cyber Asset could, depending on the configuration of the intermediate system, enable a pivot attack. Refer to the SPP RE comments regarding Reference Model 8 in response to question 5.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Please see previous comments. Texas RE encourages entities to have an inventory of their low impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CIP-003-7, Attachment 2, Section 2b, as written suggests that the Responsible Entity is required to have a list of Cyber Assets. CenterPoint Energy believes the intent of the requirement is to control physical access to the Cyber Assets used to provide electronic access control for low impact BCS.

CenterPoint Energy recommends the following edits:

"The Cyber Asset(s) that provide electronic access control(s) implemented for Section 3.1, as specified by the Responsible Entity, if any."

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	No

Document Name	
Comment	
For each asset or group of assets that contain LERC, documentation showing that communication to Low Impact BCS is confined to only that which the Responsible Entity deems necessary. Examples of this documentation could include representative diagrams or lists of the implemented electronic access controls (e.g., restricting IP addresses, ports, or services; authenticating users, air-gapping networks; terminating routable protocol sessions on a non-BES Cyber Asset; implementing unidirectional gateways).	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
The proposed revisions to the Low Impact External Routable Connectivity (LERC) definition, retirement of the Low Impact Electronic Access Point (LEAP) and associated changes to the requirements for CIP-003 Attachment 1 Section 2 and 3 represent a significant shift from the currently FERC-approved definitions and requirements. The proposed changes include identifying LERC to non-BES Cyber Assets increasing the scope. Entities are well into their implementation of the approved definitions and requirements. This fundamental shift creates regulatory uncertainty for entities and timing concerns to meet the proposed implementation schedule due to re-work and the volume of assets containing low impact BES Cyber Systems. At best, FERC approval is not likely till near the end of 2017, which will be too late for most entities' budgeting schedules for work to be completed in 2018 if the revised requirements require budget changes. It's not logical to vote yes on the non-binding poll until the requirement language is closer.	
Likes 0	
Dislikes 0	
Response	
Robert Tallman - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name LG&E and KU Energy	
Answer	No
Document Name	
Comment	
LG&E/KU believes this needs to be modified based on the change in definition.	
Likes 0	
Dislikes 0	
Response	

Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SCE agrees with and supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Erika Doot - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

In Attachment 2, Section 3, examples of evidence "such as representative diagrams or lists of implemented electronic access controls (e.g., restricting IP addresses, ports, or services; authenticating users; air -gappi implementing unidirectional gateways)" where not previously specified could be interpreted to apply some of the same requirements as for high and medium impact BES Cyber Systems. Reclamation is not clear on whether the intent of this revision is to update the requirement. Reclamation requests that the drafting team provide clarification on whether the addition of this language is intended to update R2.

Likes 0	
Dislikes 0	

Response

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer	No
Document Name	

Comment

Seattle finds the proposed concept of LERC and the associated controls to be incompetely considered and subject to numerous confusing and/or unintended consequences. If the proposed approach must be adopted, please at least clarify the following questions:

1. If there are multiple sources of LERC at an asset (site), are individual electronic access controls for a BCS required for each source of LERC, or is one blanket access control sufficient? What about the case of an asset (site) having two different sources of LERC: one source being a badge reader system connected to a company-wide network by Ethernet and the other source being a wireless business network to connect

some desktops and a printer. An air gap might be a sufficient and appropriate protection against the Ethernet-based LERC, but by itself would not be so for the wireless LERC. By extension, would every source of LERC need be identified, documented, and controlled?

2. Do the following cases represent violations for Section 3? For one, consider an asset without LERC, which has BCS that lack any capability for routable communications. If someone entered the site with a cellphone that had an activated internet hotspot (perhaps because he or she used the hotspot at home the night before and forgot it was still active), does the temporary introduction of LERC and the lack of any specified LERC control on the BCS constitute a violation? Would it still be a violation if the cellphone itself never entered the asset (site) but the hotspot range (the routable communications) did reach inside the asset (site)? For two, consider an asset (site) with LERC sourced from an ethernet business network. The local BCS is air gapped from the business network. Now if the same hotspot-enable cellphone is brought into (or nearby) the site, introducing wireless LERC, is there a violation? Would it matter if the BCS was inherently incapable of any routable communications?

3. Can prospective electronic access controls for a BCS be specified in advance of knowing the specific source of the LERC (or if there is any LERC at all)? In particular, consider the case of a BCS composed of one or more BCAs that lack the capability to support routable communications. Would it be considered compliant to simply list “air gap” for this BCS without knowing anything at all about the type and/or presence of LERC at the location (asset)?

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

See question 1 comment.

Likes 0	
Dislikes 0	

Response

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

The statement:

“Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both.”

We expect that monitoring controls will not control access in the view of NERC CMEP based on Version 5 audit approach identified in the evidence request and will not be accepted as evidence of compliance. As a result, the expectations are unclear. The language in Attachment 1 needs to be updated to permit the use of monitoring as a form of access control

Section 3

There are no measures/documentation identified for the specific case that LERC or Dial-up does not exist. The applications guideline states "[i]n the case where there is no LERC or Dial-up Connectivity, the Responsible Entity can document the absence of such communication in its low impact cyber security plan(s)." Does this mean an attestation or statement that there is no LERC or Dial-up Connectivity in an asset sufficient? If not, please provide specific examples of ompliance measures when there is no LERC or Dial-up Connectivity present.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The language in of CIP-003-6, Attachment 2, Section 3-1 does not properly restrict the applicability to the Low Impact BES Cyber Systems within an asset.

Suggested language:

Documentation, such as representative diagrams or lists of implemented electronic access controls (e.g., restricting IP addresses, ports, or services; authenticating users; air gapping, gateway, unidirectional gateways, etc.) showing that LERC at each asset or group of assets containing low impact BES Cyber Systems, has been limited to the necessary electronic access deemed necessary by the Responsible Entity to Low Impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AECI supports the revised measure, which states, “Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to: 1. Documentation, such as representative diagrams or lists of implemented electronic access controls…” Upon analysis of the text in this measure, it appears that a single representative diagram could be utilized as substantiating evidence for several BES assets that share a common configuration. If this was the intention of the SDT, it could relieve entities of added compliance burden related to documenting LERC under the proposed definition. AECI supports the new definition and this approach to demonstrate compliance.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Exelon - 6	
Answer	Yes
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Ruth Miller - Exelon - 5	
Answer	Yes
Document Name	
Comment	

See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
John Bee - Exelon - 3	
Answer	Yes
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
We agree with the proposed revisions.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Attachment 2, Section 3: Please consider using the term “isolating” or “separating” instead of or alongside the use of “air-gapping.” The strict use of the term “air-gap” implies that there are no cables whatsoever connected to a device that allows any communication to or from the air-gapped device. However, it appears that the use of air-gap in the proposed revisions is only referring to communication that is outside of the asset containing	

the low impact BES Cyber System, while there is no air-gap restriction to the Cyber Asset being connected for communication within the asset containing the low impact BES Cyber System. Exelon foresees that there could be some enforcement confusion over this nuance and recommends that the SDT clarify within the GTB to what extent air-gapping as an electronic access control is acceptable.

The revised measures posted for comment would also accommodate all of the proposed language changes presented in questions 1 and 3.

Likes 0	
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	Yes
Document Name	

Comment

We support the SDT approach of not prescribing how Responsible Entities meet the security objective. The non-exclusive examples described in the Measure are useful.

Likes 0	
Dislikes 0	

Response

Stephanie Little - APS - Arizona Public Service Co. - 5

Answer	Yes
Document Name	

Comment

AZPS is in agreement with aligning the language of the Measure to be consistent with the language of all Requirements.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Burns & McDonnell - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	Yes
Document Name	

Comment

No Comment	
Likes 0	
Dislikes 0	
Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Yvonne McMackin - Public Utility District No. 2 of Grant County, Washington - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michiko Sell - Public Utility District No. 2 of Grant County, Washington - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Johnny Anderson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Oshani Pathirane - Oshani Pathirane On Behalf of: Paul Malozewski, Hydro One Networks, Inc., 1, 3; - Oshani Pathirane	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Barnett - Exxon Mobil - 7	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - NA - Not Applicable - SPP RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no NextEra	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey Watkins - Jeffrey Watkins On Behalf of: Eric Schwarzrock, Berkshire Hathaway - NV Energy, 5; - Jeffrey Watkins	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Oliver Burke - Entergy - Entergy Services, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
ALAN ADAMSON - New York State Reliability Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 1, 5, 3; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Varnell - Tenaska, Inc. - Tenaska Power Services Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	
Document Name	
Comment	
N&ST agrees with the update to Measure M2 to CIP-003-6, Attachment 1, Sections 2 and 3.	
Likes 0	
Dislikes 0	
Response	

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	
Document Name	
Comment	
We support the comments of TransÉnergie.	
Likes 0	
Dislikes 0	
Response	
Julie Ross - Austin Energy - 3	
Answer	
Document Name	
Comment	
I support Andrew Gallo's comments.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF	

Answer	
Document Name	
Comment	
WEC Energy Group (including Wisconsin Electric and Wiscsonsin Publice Service).participated in the development of and support EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	
Document Name	
Comment	
signing on with NIPSCO comments of Sarah Gasienica	
Likes 0	
Dislikes 0	
Response	

5. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides example diagrams that illustrate various electronic access controls at a conceptual level. Do you agree with the content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

We respectfully point out that within the section "Insufficient Access Controls" of the GTB the term LEAP still appears in Reference Models 1 thru 4 and 7. This appears to be an editing error but should be rectified.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5

Answer	No
Document Name	

Comment

Due to the amibiguity of the proposed definition, the examples are confusing especially as the SDT continues to confuse Cyber Assets with Physical Assets.

Likes 0	
Dislikes 0	

Response

Emily Rousseau - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO-NERC Standards Review Forum (NSRF)

Answer	No
Document Name	

Comment

In addition to the Guidelines and Technical Basis diagrams we suggest providing a diagram to illustrate electronic access controls with an example using a multiplex system (SONET) that shares hardware and includes serial non-routable protocol to low impact BES Cyber Assets and Ethernet routable protocol to non-BES Cyber Assets. This configuration is used by many Low Impact entities. See provided diagram. Per this diagram, only the right hand side (which utilizes routable protocol) would have an associated LERC at the boundary whereas the left hand side (which utilizes serial non

routable serial protocol) would have no LERC. Note, the right and left hand side enter the asset boundary on a “shared” (carrying both routable and not routable protocol communications) Optical Fiber cable and utilize a “shared” multiplexer however since the left had side is not routable Similar to LERC Reference Model 2 in CIP-003-7, the nonroutable “low impact BES Cyber System(s) are on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s)”.

Likes 0	
Dislikes 0	

Response

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

The comment “The term “BES Asset Boundary” is capitalized in the diagrams but it is not a defined term” raises concern. Please use the proper capitalization for the defined terms to prevent confusion.

Reference Models 1 and 2 use the term LERC as defined, however the use of the term in this manner introduces confusion.

Reference Model 1 may need to clarify the use of the term air-gap with respect to wireless communications. While the vast majority of the audience will understand the concept, it may be necessary to ensure the model is understood correctly by some entities. Using the term LERC to highlight communications to non-BES equipment confuses the intent of the requirement. While the intent is clear, the diagram provided does not necessarily meet attachment 3, section 1. Specifically,

“Implement electronic access control(s) for LERC, if any, to permit only necessary electronic access to low impact BES Cyber System(s).”

One valid understanding of the requirement is that access control(s) for LERC is required. Further, the electronic access control(s) shall permit only necessary electronic access to low impact BCS. The diagram, as presented, does not have any electronic access controls on LERC. Even though clearly not the intent, the language allows this interpretation.

Reference Model 2 may need to clarify that the intent is to use a configuration technique such as private VLANs to ensure the model is not misinterpreted. Again, this may be necessary to ensure the model is understood correctly by some entities.

Reference Model 3 should clarify the intent of the firewall is to control logical ports, such as TCP and UDP ports, for inbound and outbound communications. As written in this model, it could be interpreted that any use of Windows firewall on the Cyber Asset, regardless of how effectively configured, meets the expectations of this model.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns

Answer	No

Document Name	
Comment	
ITC likes the visual depictions and the information provided in the supplemental material, however, as indicated in question #2, ITC prefers that these diagrams reflected a demarcation point to the network boundary and ther term LEAP remains effective.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
See question 1 comment.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	No
Document Name	
Comment	
If the new proposed LERC approach is deemed necessary, please include a reference model diagram for Low impact assets that clearly indicates that a routable business network, business network device (such as a printer or desktop), or any other non-BES system that is not connected to any BES Cyber System is out of scope for LERC. Please also clarify that LERC is intended to be a property of an individual BES Cyber System and not a property of an asset (site) as a whole. Please also expand the discussion of LERC and the required controls to address the issues discussed above in Measures question #4 (controls for multiple sources of LERC, temporary/incidental introduction of LERC, pre-specified anti-LERC controls).	
Likes 0	
Dislikes 0	
Response	

Erika Doot - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
In the GTB section, "Determining Asset Boundary" the concept of a "logical border" is describing a physical border for low impact facilities, and not what would normally be referred to as a "logical border." Reclamation requests that the logical border concept be maintained in this section.	
Likes 0	
Dislikes 0	
Response	

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
The Requirement 2 Attachment 1 – Section 3 as well as the Reference Models provided in the GTB require the Responsible Entitiy to list all external routable communications. We recommand focusing only on the external routable communications that could potentially cross a low impact BES network, therefore excluding all communications that are physically isolated from the low impact BES. Doing so, we recommend to remove Reference Model 1 – Physical Isolation, as it significantly increases the effort dedicated to documenting and maintaining the list of LERCs, and does not add security value on the low impact BES itself. *In addition to exclude all pure administrative communications, removing the Reference Model 1 – Physical Isolation will also allow to exclude temporary LERCs, such as data enabled cell phones or contrator wifi network, which have no reliability impact.* *The methodology implicitly suggested with CIP003-7 (and Reference Model 1) seems like a top-down approach, since all external routable communications to a low asset need to be listed to eventually identify how the low impact BCS of an asset are electronically secured.* *We currently use a bottom-up methodology, where we first identify each one of our low impact BCS, and, for each, we verify the existence of external routable communication (LERC). We then ensure an electronic access control for each existing LERC. Changing our methodology for a top-down approach represents important impacts in terms of effort, budget and capability of meeting the due deadlines.*	
Likes 0	
Dislikes 0	
Response	

Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment	
Due to the nature of the issues and concerns raised by the industry, the Guidelines and Technical Basis sections will need to be revised.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
The proposed revisions to the Low Impact External Routable Connectivity (LERC) definition, retirement of the Low Impact Electronic Access Point (LEAP) and associated changes to the requirements for CIP-003 Attachment 1 Section 2 and 3 represent a significant shift from the currently FERC-approved definitions and requirements. The proposed changes include identifying LERC to non-BES Cyber Assets increasing the scope. Entities are well into their implementation of the approved definitions and requirements. This fundamental shift creates regulatory uncertainty for entities and timing concerns to meet the proposed implementation schedule due to re-work and the volume of assets containing low impact BES Cyber Systems. At best, FERC approval is not likely till near the end of 2017, which will be too late for most entities' budgeting schedules for work to be completed in 2018 if the revised requirements require budget changes. It's not logical to vote yes on the non-binding poll until the requirement language is closer.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Good recommendation however, it does not align with the verbiage of the requirement. The Supplemental Material should give examples of strict interpretation of the requirements language.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	

Answer	No
Document Name	
Comment	
CenterPoint Energy recommends the STD to make modifications to the Guidelines and Technical Basis section to align with the proposed LERC definition as commented in Question #1.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
The SDT made a minor adjustment that is different than the rest of the standards. Starting on page 26, the header was changed from “Guidelines and Technical Basis” to “CIP-003-7 Supplemental Material”. The term “Supplemental Material” is new; Texas RE believes this is an unnecessary change and raises more questions, than simply leaving it as “Guidelines and Technical Basis”. **Requirement R2, Attachment 1, Section 2 – Physical Security Controls**, page 30, under the last paragraph it states, **“***Monitoring as a physical security control can be used as a complement or an alternative to access control*.” Texas RE suggests removing the statement “or an alternative”. Monitoring alone is not a proper form of access control. **Determining LERC Section**, page 30, Texas RE suggests diagram(s) showing LERC examples would be beneficial given the fact that all the LERC reference models are showing examples of “*various electronic access controls at a conceptual level*.” Can the assumption be made that if one the concepts is being used already, then there is LERC present? **Determining Asset Boundary**, page 31; Texas RE suggests diagram(s) showing examples of asset boundaries would be beneficial.	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No

Document Name	

Comment

Tacoma Power supports the APPA comments on this issue.

Likes 0	
Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10

Answer	No
Document Name	

Comment

The SPP RE offers the following comments with respect to the pertinent section of the Guidelines and Technical Basis: (1) The second sentence of the first paragraph of the guidance for Requirement R2, Attachment 1, Section 2 should be clarified that the reference to “these Cyber Assets” is referring to the Cyber Assets that implement the electronic access control(s). While it should be intuitively obvious, the sentence in its entirety is somewhat awkward and confusing and could be restated for clarity. (2) The last paragraph of the guidance for Requirement R2, Attachment 1, Section 2 states, in part, that monitoring as a physical control can be used as an alternative to access control. The SPP RE disagrees, noting that monitoring is not an effective means to deter unauthorized access, especially when there is low to no probability of a rapid response to an intrusion. A remotely monitored camera or sensor, coupled with a significantly time-delayed response, does not control access, whereas a simple lock on a door is an effective deterrent. Neither will assure against unauthorized access, but the locked door at least is a barrier than must be defeated whereas a monitoring system in the absence of physical access controls offers no impediment to entry. (3) The third sentence of the first paragraph of the discussion on determining the asset boundary allows the Registered Entity to determine the asset boundary based on the physical location of networked Cyber Assets. In the instance where there are networked Cyber Assets (same Local Area Network) well outside of the fence line of the asset, such as cooling water well heads miles away from a generating plant, the Registered Entity would be allowed to define the asset boundary to encompass the remote sites without regard to being able to protect the remote Cyber Assets or the communication paths. (4) The SPP RE does not believe that Layer 2 Virtual LANs, as suggested to be permissible by LERC Reference Model 2, can provide logical network segmentation sufficient to assure no communication can occur between the Non-BES Cyber Assets and the Low impact BES Cyber Systems depicted in the diagram. Network isolation needs to be accomplished at Layer 3, with appropriate access controls. (5) LERC Reference Model 7 calls for authenticating a new session before establishing a connection to a Low Impact BES Cyber System. It is not clear whether this reference model is envisioning an intermediate system (jump host) without all of the accompanying controls required of an Intermediate System for High and Medium impact BES Cyber Systems, or more like the AAA authentication performed upon session initiation by a firewall or other similarly capable device such as that envisioned by CIP-005-3, Requirement R2.4. Clarification is requested. (6) LERC Reference Model 8 needs to clarify that any traffic between the Non-BES Cyber Asset in the DMZ and the Low Impact BES Cyber System must go through the access control device. A dual-homed (back end network) environment that allows unrestricted, direct access between the DMZ Cyber Asset and the BES Cyber Asset should be strictly prohibited whether or not IP Forwarding is enabled. Such a configuration enables a pivot attack that would essentially bypass the protective controls put into place to protect the Low impact BES Cyber System.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	
Comment	
Due to our other concerns raised in these comments, the Guidelines and Technical Basis will also need to be edited.	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	
AZPS is opposed to including example diagrams as part of the Guidelines and Technical Basis (GTB) section of the standard due to the fact that standards may not be updated frequently enough to reflect the most recent technology changes/options. AZPS is in agreement that example diagrams are a useful resource and would recommend inclusion of such in general standard development guidelines documentation, which would provide the ability for more efficient operational changes. In regards to the specific Reference Models, AZPS offers the following: Reference Model 2 – AZPS does not believe this diagram meets the Requirement as there is no security device/function depicted. AZPS also respectfully requests that the GTB section not contain additional or conflicting language to the requirements to avoid confusion or misinterpretation. Attachment 1, Section 3.1 states that entities must “[i]mplement electronic access control(s) for LERC, if any, to permit only necessary electronic access **to** low impact BES Cyber System(s)” (CIP-003-6 Redline, Page 22, emphasis added). However, GTB Requirement R2, Attachment 1, Section 3 states that electronic access controls are required when “external routable protocol communication (LERC) or Dial-up Connectivity is present **to or from** the asset containing the low impact BES Cyber System(s)” (CIP-003-6 Redline, Page 30, emphasis added). AZPS recommends aligning the language between these two statements.	
Likes 0	
Dislikes 0	
Response	
Christy Koncz - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG	
Answer	No
Document Name	
Comment	

PSEG agrees with and supports EEI's comments.

Likes 1	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

1. Please eliminate the concept of LERC. All electronic communications should have access controls. Reference Model 1 illustrates that absence of routable connectivity is an example of an electronic access control for communications. It also illustrates that the use of non-routable communications functions as an electronic access control. The sections “Determining LERC” and “Determining Asset Boundary” would no longer be needed if the LERC definition is eliminated. Add a discussion of secure deployment of routable time-sensitive communications such as IEC 61850.

2. In general, the Reference Models do a good job of illustrating that entities have flexibility in where and how they choose to implement electronic access controls. However, Reference Model 5 shows communication through a “cloud” that implies an unprotected or shared network. Even if communication is over a VPN, the BES Cyber Systems located at the BES assets could be exposed to probes for open ports and vulnerabilities. Please consider removing the “cloud” graphic and change the final sentence to “Care should be taken that electronic access to the networks at the BES asset where BES Cyber Assets reside can only be through the device controlling electronic access at the centralized location.”

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

In addition to the Guidelines and Technical Basis diagrams we suggest providing a diagram to illustrate electronic access controls with an example using a multiplex system (SONET) that shares hardware and includes serial non-routable protocol to low impact BES Cyber Assets and Ethernet routable protocol to non-BES Cyber Assets. This configuration is used by many Low Impact entities.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
In addition to the Guidelines and Technical Basis diagrams we suggest providing a diagram to illustrate electronic access controls with an example using a multiplex system (SONET) that shares hardware and includes serial non-routable protocol to low impact BES Cyber Assets and Ethernet routable protocol to non-BES Cyber Assets. This configuration is used by many Low Impact entities.	
Likes 0	
Dislikes 0	
Response	

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	No
Document Name	
Comment	
Revise the GTB section of the standard to correspond with the proposed revisions in the alternate proposal (see question 3). Also incorporate text from FERC Order 822 paragraphs 67, 69 and 74 regarding implementation of the “layer 7 application layer break” and how NERC clarified it. Revise the posted Reference Models to reflect the proposed retirement of LERC.	
Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry
Dislikes 0	
Response	

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy supports the comments submitted by Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	

Southern Company generally supports the comments filed contemporaneously by the Edison Electric Institute ("EEI"). Southern Company appreciate the opportunity to support EEI's Comments as well as to provide the additional comments regarding references to wireless on page 27, CIP-003-7 Supplemental Material, Part 1.1.2, Organization Stance on the Use of Wireless Networks, Southern Company would prefer further statements and or guidance concerning wireless connectivity.

As proposed, the CIP-003-7 standard implies that wireless protocols should be identified for all wireless communications which cross the Asset's boundary, including both inbound and outbound. Additional clarification should be provided that wireless communications which are configured for the BES Cyber System or associated BES Cyber Asset should be documented. All other wireless communications not configured for a BES Cyber System or associated BES Cyber Asset contained within the defined boundary should be considered out of scope.

Likes 0	
Dislikes 0	
Response	

Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	

The diagrams show examples of "LERC" where it does not exist, which is confusing the definition of LERC with general "external routable connections" (in other words, connections that only include devices that are non-BES Cyber Systems). The definition of LERC is "Low Impact External Routable Communication". One must have a Low Impact BES Cyber System in order to have LERC. Therefore there cannot be LERC without a Low Impact BCS, and therefore you cannot have, as stated in the technical guidance, LERC without connectivity to low impact BES Cyber Systems. If this correction is not made, the simple act of taking a cellphone into a "BES asset" would immediately create LERC. This is unworkable. We understand the challenge of defining LERC, but the focus must remain on low impact BES Cyber Systems and not drag in additional devices that have no bearing on the security of the BES Cyber System. The fact that a computer with an external network connection is in the same room as a BES Cyber System has zero bearing on the security of the BES Cyber System unless the devices are connected in some fashion. Any time there is an "air gapped" network that is sufficiently documented showing zero external connections outside of an asset boundary, that should be all that is required for compliance.

Reference Model 1 does not properly indicate a risk to the BES, and misuses the term LERC.

Reference Model 2 does not demonstrate "LERC" as the Low Impact BES Cyber Systems do not have external routable connectivity. If the SDT wishes to indicate that VLANs or other such technologies are insufficient as protections between logical networks, this information needs to be provided in a

broader context than just switches. Any type of packetized network device is inherently just as risky as a VLAN tag on a properly configured managed switch. However, the mere presence of external routable connectivity on 'any' VLAN on the switch does not constitute LERC.

Reference Model 5, while perhaps useful in some scenarios, can cause extreme problems in others. If an entity were to designate a BES Asset Boundary in a generation plant using the smallest footprint possible (and thereby increasing security due to controlling smaller areas where the BES Cyber Assets actually reside), it would no longer allow the plant to operate. The reason an entity would NOT choose to use the fence line, as suggested in the Supplemental Material, is because this could include additional non-BES Cyber Assets (such as cameras, phones, corporate workstations, etc.) that have no bearing on the security of the BES Cyber System(s). So by choosing a smaller footprint it would prevent the plant from properly communicating on its LAN without having the entire system re-architected. It would then also introduce a single point of failure which would in turn reduce reliability. There should be no additional compliance burden placed on the entity to show how they are protecting "LERC" if there is no bearing on the BES Cyber System. There should also be consistency applied to the Reference Models in order to reduce confusion.

Reference Model 5 also includes the term "Non BES Cyber System" as part of the reference model. This should at least state "Non BES Cyber Asset" to be consistent with the other diagrams.

Reference Model 8 shows a BES Asset Boundary that should only include Low Impact BES Cyber Systems and any other devices on the same network segment. "DMZ" networks should be outside of the BES Asset Boundary. While we agree that the "jump host" idea can be a way to increase security, it can also be abused if it is not properly configured.

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

The Guidelines and Technical Basis section needs to be reviewed for consistency in numerous places. There are terms that are capitalized that are not NERC defined terms (BES Asset Boundary, Non BES Cyber System). A review should also be done to make sure the reference models shown are what is needed for the industry to apply in their environments.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No

Document Name	

Comment

Pg 29 Under Requirement R2, Attachment 1, Section 2 – Physical security controls:

“If these Cyber Assets are located within the BES asset and inherit the same controls

outlined in Section 2, this can be noted by the Responsible Entity in either its policies or cyber

security plan(s) to avoid duplicate documentation of the same controls.” This section is confusing and makes no sense. The logic seems circular in protecting the asset.

Pg 31 Determining Asset Boundary

We would suggest to the drafting team to revise the title of the sections to ‘Determining BES Asset Boundary’ for consistency through out the documentation.

LERC Refereence Model 5 – Centralized Network-based Inbound& Outbound Access Permissions

“Care should be taken that electronic access to or between each BES asset is through the electronic access controls at the centralized location.”

We would suggest stronger language instead of ‘Care should be’, this is not allowed under the definition of LERC and should be stated as so.

LERC Refereence Model 8 – Session Termination and Model 7 User Authentication

This model is an example of a piviot attack metntioned for #4. The flow of traffic must stop at the non-BES Cyber Asset and only communicate with the Low-Impact BES Cyber System, otherwise what happens if that non-BES Cyber Asset is compromised?

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	

Comment

FMPA supports the comments of American Public Power Association.

Likes 0	
Dislikes 0	

Response

Michael Buyce - City Utilities of Springfield, Missouri - NA - Not Applicable - SPP RE	
Answer	No
Document Name	
Comment	

Page 26: The header reads, “Supplemental Material”, but the main heading on the page reads, “Guidelines and Technical Basis.” Was it the intent of the SDT to replace the Guidelines and Technical Basis with Supplemental Materials, or make Guidelines and Technical Basis one part of the Supplemental Material? It is the only first-level heading in the Supplemental Material.

Page 29: Requirement R2, Attachment 1, Section 2 – Physical Security Controls, part 1 of the first sentence reads, “The asset or the locations of low impact BES Cyber Systems…” might be better phrased as, “The asset or the locations [containing] low impact BES Cyber Systems…” This should keep with the consistency throughout the requirements.

The Supplemental Material for the proposed CIP-003-7 requirements introduces the phrase “BES assets,” (**Requirement R2, Attachment 1, Section 3 – Electronic Access Controls** (page 30)). This phrase is used interchangeably within the Supplemental Material, and in some instances within the same sentence. Since the phrase, “Assets containing low impact BES Cyber Systems,” is consistently used throughout the currently approved CIP requirements, would the SDT reconsider the use of “BES assets?”

Page 31: The first sentence reads, “As LERC is a BES asset level attribute, it involves a determination by the Responsible Entity of a BES asset boundary for their assets containing low impact BES Cyber Systems.” Considering the recommendation above, to avoid reduncancy, and provide clarity, would the SDT consider revising the first sentence? Below are two recommendations.

- “As LERC is an attribute of an asset containing low impact BES Cyber Systems, it involves a determination of a boundary, by the Responsible Entity, for each asset containing low impact BES Cyber Systems.” or,

- “LERC is an attribute of an asset containing low impact BES Cyber Systems. The Responsible Entity determines appropriate boundary for each asset containing low impact BES Cyber Systems.”

Page 31: The last sentence in the second paragraph reads, “However, this also means that LERC can exist for a BES asset even if there is no routable protocol connectivity to any low impact BES Cyber System within the BES asset.” Was the intention of the SDT to mean “routable protocol communication” in this instance?

There is somewhat of an inconsistent use of the terms: (1) Necessary access; (2) “Necessary” access; and (3) “Necessary electronic access.” Attachment 1, Section 3, part 3.1 uses the phrase “Necessary electronic access.” On page 32, “Necessary” appears within quotes twice. On page 32 in the Concept Diagrams section, and in some of the reference models, the phrase “necessary access” is used when referring to “necessary electronic access.” Could the SDT consider using the phrase “necessary electronic access” when applicable?

The phrases ‘from the LERC’ and ‘across the LERC’ may cause some confusion.

Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No

Document Name	

Comment

N&ST believes that the diagrams in the revised Guidelines and Technical Basis section of the standard are vague and incomplete. In particular, the application of controls is mentioned, but the placement of the control on an individual Cyber Asset – or interface on a Cyber Asset – is not included in the diagram, clouding the ability of the diagram to communicate the intent of the discussion of the placement of the control. N&ST suggests that for each diagram, the exact placement of each control should be indicated. In addition, N&ST suggests that the legend at the bottom of each drawing should be tailored to the types of communications represented by the diagram to support clarity of the relevance and extent of the controls.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	No
Document Name	

Comment

Exelon appreciates the details within the GTB and suggests some further clarifications:

1. The discussion of Requirement R2, Attachment 1, Section 3 -- Electronic Access Controls should be explicit in stating that the determination of the "necessary" electronic access to low impact BES Cyber Systems should be within the discretion of the Responsible Entity, rather than simply "as determined by the Responsible Entity." A dispute between a Compliance Enforcement Authority and a Responsible Entity over whether certain electronic access is "necessary" should not be grounds for finding noncompliance with the Standard. The guidance should be modified to state "The control(s) **will be considered to must** allow only “necessary” access as determined by the Responsible Entity, **if the Responsible Entity can and they need to be able to** explain **the its** reasons for **its decision to identify the** electronic access permitted with **its their** electronic access controls." Additionally, the documentation of the determination can be at a policy or procedure level and is not intended to be at an individual BES asset or low impact BES Cyber System level.

2. If the concept of the “asset boundary” is retained, the section on Requirement R2, Attachment 1, Section 3 -- should leave the identification of the “asset boundary” to the Responsible Entity. As written, the GTB discussion does not sufficiently emphasize the entity determination of the “asset boundary” and help prevent a finding by the Compliance Enforcement Authority that a different “asset boundary” should have been selected. The discussion should end with the statement that "The foregoing list is not exhaustive, and Responsible Entities have the flexibility to identify the “asset boundary” they consider appropriate for their operations."

1. LERC Reference Model 2 - Logical Isolation appears to show a routable protocol into and out of the portion of the network containing the low impact BES Cyber Systems, but the description states that the illustration shows how routable protocol communications into and out of the network containing the low impact BES Cyber Systems are prevented. The diagram should be clarified to match the description.

1. LERC Reference Model 5 - Centralized Network-based Inbound & Outbound Access Permissions states that "The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s)." Depending on the implementation, this

may be a significant change from the current CIP-003-6 and this language should be incorporated in the main body of the diagram, rather than only a reference model. The GTB should state that "This Standard does not require the electronic access control(s) required by Attachment 1 section 3.1 to reside or be applied inside the asset containing the low impact BES Cyber System. The geographic location of **any** Cyber Asset providing electronic access control required for compliance with Attachment section 3.1 is irrelevant so long as the electronic access controls permit only necessary electronic access to the low impact BES Cyber System." The currently approved Version 6 language is specific to the placement of a LEAP being allowed at a location other than the asset containing the low impact BES Cyber System. However, the other currently approved reference models identify that the remaining electronic access controls are applied within the asset containing the low impact BES Cyber Systems. Exelon recommends the SDT clarify if it is permissable that any electronic access controls be applied at a location other than the asset containing the low impact BES Cyber Systems.

1. Exelon supports inclusion of the diagrams in the GTB. We request an additional Reference Model to build on the Reference Model 1 scenario to show routable communication to a BCS and a non-BCS but with the electronic access control going only to the BCS in the asset.

1. Exelon is concerned with the use of the term “air-gap” in the construct of the proposed revisions. The strict use of the term “air-gap” implies that there are no cables whatsoever connected to a device that allows any communication to or from the air-gapped device. However, it appears that the use of air-gap in the proposed revisions is only referring to communication that is outside of the asset containing the low impact BES Cyber System, while there is no air-gap restriction to the Cyber Asset being connected for communication within the asset containing the low impact BES Cyber System. Exelon foresees that there could be some enforcement confusion over this nuance and recommends that the SDT clarify within the GTB to what extent air-gapping as an electronic access control is acceptable.

Proposal: If the Proposed language in Questions 1 and 3 is adopted, the GTB will need to be updated accordingly (i.e. remove assert boundary discussion).

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb

Answer	No
Document Name	

Comment

Concern—CIP LERC Reference Model 1, as offered, basically illustrates any routable protocol crossing the BES Asset Boundary is converted into a BES Cyber Asset. If that is the intent, that reinforces our concerns regarding the potential expansive scope of applicability inherent in the proposed LERC term.

We believe LERC should only reflect connections to low impact BES Cyber Systems and, as such, we question how the diagram has a LERC since a LERC connection is not made to a BES Cyber Asset or System.

Proposal

As previously offered, a modification to the proposed LERC term would temper the potential scope of applicability to only routable protocols connected to low impact BES Cyber Systems.

“A routable protocol communication that crosses the boundary of an asset connected to one or more low impact BES Cyber Systems…”

Incorporating this proposal would require modifying the Model No. 1 illustration or removing it from the GTB.

Likes 0	
Dislikes 0	

Response

Tim Kucey - PSEG - PSEG Fossil LLC - 5

Answer	No
Document Name	

Comment

PSEG supports EEI comments

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

NRECA appreciates the efforts to improve the GTB for R2, and has the following requests for additions to the GTB. First, it would be beneficial if the GTB were revised to show scenarios of dial-up connectivity at low impact facilities. Next, the GTB capitalizes “BES Asset Boundary” in the diagrams, and since this is not a NERC-defined term, it should be corrected to “BES asset boundary.” Lastly, based on all of the comments submitted by NRECA and others, the GTB will need to be updated to address changes made by the SDT.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3

Answer	No

Document Name	
Comment	
Cowlitz PUD supports APPA comments.	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	No
Document Name	
Comment	
GCPD appreciates the SDTs efforts to clarify the intent of the CIP-003-7 Standard to low impact BES Cyber Systems. However, we are constantly reminded that we will be audited to the Standard Requirement and NOT the Guidelines and Technical Basis. As such, any clarifications to definitions and applicability should be included in the body of the Standard Requirements. Not in an unenforceable section of “supplemental material”.	
Likes 0	
Dislikes 0	
Response	
Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker	
Answer	No
Document Name	
Comment	
Please see the answer to question 3 above.	
Likes 0	
Dislikes 0	
Response	
Johnny Anderson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	

Comment
The wording related to what devices will require the physical protection is unclear. As it reads it seems the SDT is saying protect a “LEAP” that no longer exists but it is unclear what will be expected to protect these potentially varied electronic access controls.

Likes 0	
Dislikes 0	

Response

Michiko Sell - Public Utility District No. 2 of Grant County, Washington - 1	
Answer	No
Document Name	

Comment
• GCPD appreciates the SDTs efforts to clarify the intent of the CIP-003-7 Standard to low impact BES Cyber Systems. However, we are constantly reminded that we will be audited to the Standard Requirement and NOT the Guidelines and Technical Basis. As such, any clarifications to definitions and applicability should be included in the body of the Standard Requirements. Not in an unenforceable section of “supplemental material”.

Likes 0	
Dislikes 0	

Response

John Bee - Exelon - 3	
Answer	No
Document Name	

Comment
See Exelon TO Response

Likes 0	
Dislikes 0	

Response

Ruth Miller - Exelon - 5	
Answer	No
Document Name	

Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Exelon - 6	
Answer	No
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA's position is that the intent of Order 822 is not met by the proposed v7. FERC directed NERC to clarify the definition of LERC. From the GTB on Determining LERC: "With LERC being a BES asset level attribute, it is used as a higher level filter to exclude from further consideration those assets containing low impact BES Cyber Systems that have no routable protocol communications to them from outside the BES asset. Responsible Entities can then concentrate their electronic access control efforts on those BES assets that do have LERC. However, this also means that LERC can exist for a BES asset even if there is no routable protocol connectivity to any low impact BES Cyber System within the BES asset." The diagrams are great illustrations on the diversity, complexity, and ultimately all over the map levels of vulnerability that will represent the state of implementing some form of access control for low BES assets.	
Likes 0	
Dislikes 0	
Response	

Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
Please include a reference model diagram for Low impact assets that clearly indicates that a routable business network and/or business network device (such as a printer or desktop) not connected to any BES Cyber System is out of scope for LERC. Please also clarify that LERC is intended to be a property of an individual BES Cyber System and not a property of an asset (site) as a whole.	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	
LERC Reference Model 1 is based on a general definition of “communications” traversing a LERC boundary as opposed to “connectivity” to a BES Cyber System with an external routable protocol. In addition, “air gap” is not appropriately defined nor a sufficient term in defining segmentation.	
Likes 0	
Dislikes 0	
Response	
Yvonne McMackin - Public Utility District No. 2 of Grant County, Washington - 4	
Answer	No
Document Name	
Comment	
See commentary submitted by Michiko Sell, Public Utility District No. 2 of Grant County, WA.	
Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC

Answer	Yes
Document Name	

Comment

Is there thought on using encryption for LERC?

For reference Model 7, all previous model focused on acceptable approaches where 7 is more an approach that is NOT acceptable or would require some careful configurations. Consider highlighting the last sentence that indicates this difference in approaches or note that additional controls may be necessary in some way. Consider putting this Model at the end with a different header;

Likes 0	
Dislikes 0	

Response

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison

Answer	Yes
Document Name	

Comment

Where applicable, we recommend each Reference Model show the “routable protocol data flow” using the symbols provided.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Burns & McDonnell - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	Yes
Document Name	

Comment

As noted in the comment for Question 3, Burns & McDonnell believes additional clarity on to what extent non-BES Cyber Systems (BCS) should be documented, although that does not fully apply to the diagrams.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Where applicable, we recommend each Reference Model show the “routable protocol data flow” using the symbols provided.

Within the section "Insufficient Access Controls" of the GTB the term LEAP still appears in Reference Models 1 thru 4 and 7. This appears to be an editing error.

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1

Answer	Yes
Document Name	

Comment

Hydro One supports comments submitted by NPCC RSC.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	Yes
Document Name	

Comment

We agree with the proposed revisions.

Likes 0	
Dislikes 0	

Response

Oshani Pathirane - Oshani Pathirane On Behalf of: Paul Malozewski, Hydro One Networks, Inc., 1, 3; - Oshani Pathirane

Answer	Yes
Document Name	

Comment

Hydro One Networks Inc. supports the NPCC RSC's comments on this question in its entirety.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Where applicable, we recommend each Reference Model show the “routable protocol data flow” using the symbols provided.

Within the section "Insufficient Access Controls" of the GTB the term LEAP still appears in Reference Models 1 thru 4 and 7. This appears to be an editing error.

Likes 0	
Dislikes 0	

Response

Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	Yes
Document Name	

Comment

Tri-State appreciates the example diagrams and finds them very helpful. However, we would benefit from a few clarifications/additions: 1) Could you please add one or two that incorporate/reflect Dial-up access? 2) Can you please clarify if “Dial-up” is equivalent to “serial non-routable protocol”, as depicted in Reference Model 1. 3) Can you please clarify whether Dial-up has to have an air gap if non-BES Cyber Assets might be accessible over the same phone system.

Likes 0	
Dislikes 0	

Response

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy

Answer	Yes
Document Name	

Comment

OCC found the nine examples provided in the GTB section of CIP-003-7 to be helpful and technically accurate. We appreciate the project team’s efforts to provide useful information that will provide guidance and help with our compliance efforts. We expect to reference the examples as support for the strategies employed to protect our Low-Impact BES Cyber Systems.

FERC attributes a great deal of importance to the GTB section. In fact, their directive to modify CIP-003 was based on one example in the GTB (related to Layer 7 application layer breaks) that they believed should be implemented into the requirements. If the Commission finds the GTB to be this compelling, then CEAs should be prepared to find an entity’s program acceptable when implemented in accordance with the GTB.

Cyber protections and modes of attack are evolving rapidly – and protections considered adequate in 2016, may not be in 2018. However, it is impossible for anyone to anticipate a previously unknown hacking strategy, or to immediately upgrade the protective approach once one occurs. Maybe this means that definitive protections must be added to the GTB in an expedited, but controlled manner – the consideration that FERC has recently requested for whitelisting based on the findings from the Ukraine incident may provide a good test case. Everyone understands the urgency, but is it inappropriate to hold entities responsible to expectations that may change based on the most recent cyber event or the interpretation by an audit team.

Likes 0	
Dislikes 0	

Response

John Varnell - Tenaska, Inc. - Tenaska Power Services Co. - 6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 1, 5, 3; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Tallman - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name LG&E and KU Energy	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Oliver Burke - Entergy - Entergy Services, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeffrey Watkins - Jeffrey Watkins On Behalf of: Eric Schwarzrock, Berkshire Hathaway - NV Energy, 5; - Jeffrey Watkins	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	
Document Name	
Comment	

signing on with NIPSCO comments of Sarah Gasienica

Likes 0	
Dislikes 0	

Response

Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF

Answer	
Document Name	

Comment

WEC Energy Group (including Wisconsin Electric and Wiscsonsin Publice Service).participated in the development of and support EEI's comments.

Likes 0	
Dislikes 0	

Response

Julie Ross - Austin Energy - 3

Answer	
Document Name	

Comment

I support Andrew Gallo's comments.

Likes 0	
Dislikes 0	

Response

Roger Dufresne - Hydro-Qu?bec Production - 5

Answer	
Document Name	

Comment

We support the comments of TransÉnergie.

Likes 0	
Dislikes 0	
Response	

6. Implementation Plan: The SDT revised the Implementation Plan such that it establishes a single effective (compliance) for the revisions made to Sections 2 and 3 of Attachment 2 in CIP-003, which will be the later of September 1, 2018 or the first day of the first calendar quarter that is nine (9) calendar months after the effective date of the applicable governmental authority's order approving the standard and NERC Glossary term, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If not, please provide the basis for your disagreement and an alternate proposal.

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

PacifiCorp supports comments submitted by Edison Electric Institute. Also, the language in the definitions and CIP-003-7 currently out for vote is a substantial rewrite of the requirements as approved by FERC. PacifiCorp cannot afford to wait to begin implementation until a revised standard is approved by FERC, meaning that any approved version that does not allow PacifiCorp to leverage work efforts already completed in alignment with the current FERC approved standard would lead to duplicative effort and costs. Any attempt to compress the overall timeline for implementation could results in a negative impact to the reliability of the bulk electric system.

Likes 0	
Dislikes 0	

Response

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray

Answer	No
Document Name	

Comment

Entities have been working towards an implementation plan under the existing definition of LERC and Connectivity, likely resulting in a small number of substations that would actually have LERC. The new definition of LERC addressing Communications brings in all substations containing Low Impact BES Cyber Assets, substantially changing the scope, budget, resources, and schedule to be compliant.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

PacifiCorp supports comments submitted by Edison Electric Institute. Also, the language in the definitions and CIP-003-7 currently out for vote is a substantial rewrite of the requirements as approved by FERC. PacifiCorp cannot afford to wait to begin implementation until a revised standard is approved by FERC, meaning that any approved version that does not allow PacifiCorp to leverage work efforts already completed in alignment with the current FERC approved standard would lead to duplicative effort and costs. Any attempt to compress the overall timeline for implementation could results in a negative impact to the reliability of the bulk electric system.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Because of the increase in scope, BPA suggests a longer implementation period will be required. Due to the need for a complete inventory to be performed, BPA is unable to estimate the amount of time required to implement.

Likes 0	
Dislikes 0	

Response

Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	No
Document Name	

Comment

Tri-State partially agrees with this proposal. We appreciate the SDT attempting to align the effective dates and establish a single compliance date, but we believe the implementation of CIP-003-6 Attachment 1, Sections 2 and 3, should be deferred/ not enforced. The issue is that the implementation approach for many in the industry would require a significant change under CIP-003-7. This is compounded by large number of BES assets that would be impacted. It seems futile to use significant amounts of resources to prepare for implementation of these sections under the CIP-003-6 standard considering there will be an upcoming shift in direction under the CIP-003-7 requirements. We understand that the SDT cannot request that this portion of CIP-003-6 be deferred; instead we encourage and recommend that NERC staff request a deferral from FERC (or no enforcement) of the implementation of CIP-003-6 Attachment 1, Sections 2 and 3.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
NRG supports the comments submitted by NPCC (Ruida Shu on 9/6/16): Recommend September 1, 2019 because of budget cycles and configuration changes impacting implementation provisions for early adoption of version 7 to align with version 6's enforcement.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Exelon - 6	
Answer	No
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Ruth Miller - Exelon - 5	
Answer	No
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	

Response	
John Bee - Exelon - 3	
Answer	No
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Johnny Anderson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
The change to LERC is significant as well as the approach that will need to be taken in CIP-002 for low impact assets. A longer implementation lead time which would include a minimum of twelve to eighteen months in the event the drafting/approval process takes longer than anticipated is recommended.	
Likes 0	
Dislikes 0	
Response	
Oshani Pathirane - Oshani Pathirane On Behalf of: Paul Malozewski, Hydro One Networks, Inc., 1, 3; - Oshani Pathirane	
Answer	No
Document Name	
Comment	
Hydro One Networks Inc. supports the NPCC RSC's comments on this question in its entirety.	
Likes 0	
Dislikes 0	
Response	

Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker	
Answer	No
Document Name	
Comment	
We believe 9 months is not enough time to effectively implement Sections 2 and 3 of Attachment 2 in CIP-003 simply because of the voluminous amont of our assets affected by the updated requirements. That stated, we believe a minimum of 24 calendar months following FERC approval is needed. We are supportive of a single date range for complying with Sections 2 and 3. However, we believe it should be clear that CIP-003v6 Attachment 1 Section 2 and 3 do not need to be implemented until the effective date of v7.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports APPA comment.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
NRECA is concerned that nine months is not adequate time for Responsible Entities to assess and implement their compliance program as currently drafted in the revised definition and standard. The Responsible Entities will have significant work to do to survey every BES asset that contains a low impact BES Cyber System and then to comply with the standard requirements. NRECA recommends revising the nine month timeframe to twenty-four months. This extension of time will allow Responsible Entities to focus on the more critical high and medium impact BES assets earlier, while providing extra time for implementation related to low impact BES assets. NRECA is also concerned that Responsible Entities will be working toward compliance with CIP-003-6 while there is potentially significant revisions forthcoming in a Version 7. In order to prevent the inefficient use of Responsible Entity resources, NRECA recommends that the SDT consider revising	

the implementation plan to state that compliance with CIP-003-6 will be deferred and replaced by CIP-003-7 and its associated implementation plan and effective date. If this is outside the scope of work for the SDT, we encourage the SDT to inform NERC leadership of this issue and the actions NERC should take to address this issue. Lastly, for the reasons stated above and in light of the potential for further changes to CIP-003-6 based on comments submitted, NRECA does not support the currently proposed implementation plan.	
Likes 0	
Dislikes 0	
Response	
Tim Kucey - PSEG - PSEG Fossil LLC - 5	
Answer	No
Document Name	
Comment	
PSEG supports EEI and NPCC TFIST comments	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
We do not agree with this proposal. We agree that a single effective date for the proposed revisions is necessary. However, Registered Entities have already incurred significant infrastructure and labor costs to implement various solutions that address the present LERC definition. The proposed Implementation Plan also does not acknowledge current efforts made by Registered Entities to address Low Impact BES Cyber System Electronic Access Points (LEAPs). We believe a new effective date should be proposed to account for identifying acceptable solutions, procuring new infrastructure, and installing these modifications on Registered Entity systems. We suggest the latter of September 1, 2019, or the first day of the first calendar quarter that is 18 calendar months after FERC's approval of the standard and NERC Glossary term.	
Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	

Concern. What is being proposed does not consider the challenge of the tasks required or the time needed to implement. Also, it is dependent on the scope created by the eventually accepted and approved LERC definition and CIP-003-7. In light of these variables, additional time is required beyond the proposed Implementation Plan, likely 24 months.

Basis. Entities are already juggling multiple initiatives and implementation of CIP versions 5 and 6 Standards. Additionally, the ONP side of the NERC Standards is seeing material changes and revisions. With many new and revised Standards still freshly borne, the implications and impacts they have or will have on BES security and operations are unknown. Establishing an implementation timeline needs to consider what currently is happening in the CIP and ONP spaces and how they will be impacted by the introduction of additional Standards that likely expand scope, with the potential of converting thousands of assets to BES Cyber Assets.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1	
Answer	No
Document Name	
Comment	

: Exelon appreciates the SDT's attempt to group the deadlines and provide a simple approach to the deadlines. However, Exelon has three concerns:

1. Nine months is not sufficient time for Responsible Entities to assess BES assets and implement a compliance program for the modified definition and revised standard. Substantial new work will be needed beyond updates to procedures or other documentation related to the compliance program. Responsible Entities will have to survey every BES asset they own that contains a low impact BES Cyber System, define the asset boundary, identify the routable protocol connections to the BES asset, document whether any of the routable connections communicate to or from a low impact BES Cyber System across the asset boundary and then identify the appropriate electronic access controls, if needed. The implementation plan should provide for at least 18 months and preferably two years for Responsible Entities to reach full compliance to allow for scheduling site visits, reviews of the communications, determinations of appropriate electronic access controls as well as procurement, testing and implementation project timeframes. Please consider the following suggested wording: "Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-7 and the NERC Glossary term Low Impact External Routable Communication (LERC) share become effective on the later of September 1, 2018 or the first day of the first calendar quarter that is twenty-four (24) calendar months after the effective date of the applicable government authority's order approving the standards and NERC Glossary term,

or as otherwise provided for by the applicable government authority." Given the inherent "low impact" nature of these BES assets, a longer implementation period should be acceptable and in the interest of reliability.

2. It is possible that FERC will not approve CIP-003-7 and its implementation plan in time to allow Responsible Entities to transition to CIP-003-7 without first having to implement CIP-003-6. This would be wasted effort and we do not believe that it is the intent or desire of the SDT or the regulators. The SDT could address this as it did for the overlap of V4 and V5. The implementation plan specifically stated that V4 would not become effective, even though the V4 implementation date would have occurred in the interim. "Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan."

3. Under the proposed Implementation Plan, CIP-003-7, R1.2.3 will become effective April 1, 2017. A plan for LERC will still be in development to accommodate the revised LERC definition and requirements. Entities will be required to develop a plan for LERC according to the CIP-003-6 language. This duplication of effort is not beneficial and it is a drain on the resources responsible for reliability and security.

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 9; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Thomas Parker, Fort Pierce Utilities Authority, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	

Comment

FMPA supports the comments of American Public Power Association.

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Depending on the outcome of the final draft, the Implementation Plan may need to be adjusted to allow more time for the changes.

Likes 0	

Dislikes 0	
Response	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	
Given the fundamental issues in the current draft, significant confusion by entities is likely to occur. Prior to supporting the implementation, these issues need to be addressed.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company is a member of the Edison Electric Institute (“EEI”) and generally supports EEI’s comments that are being submitted in response to the proposed modifications.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
Hydro One supports comments submitted by NPCC RSC.	
Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy supports the comments submitted by Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO

Answer	No
Document Name	

Comment

The proposed changes create an expansion in scope to include evidence for LERC to non-BES Cyber Assets. Entities must continue implementation with the FERC-approved requirements until such time as the proposed revisions are approved, which at best would be late in 2017. Entities work to implement the currently approved requirements will need to be re-worked based on the new revisions with likely only nine months to complete the re-work for up to thousands of assets containing low impact BES Cyber Assets. By mid-2017, it will be too late to budget for different equipment purchases for work to be done in 2018 if the revisions require any. Therefore, the proposed implementation schedule does not allow enough time to implement the proposed changes. Instead of the latter of Sept. 1, 2018, or 9 months after FERC approval, it should be 24 months after FERC approval.

Alternate proposal: The alternate proposal in question 3 would leverage and extend work on the FERC-approved requirement for lows. Entities could implement lows as approved with certainty work already completed would not have to be redone and would be compliant with revisions that would have later effective dates to address FERC's directive. With this proposal that would minimize re-work, the implementation plan could be the latter of Sept. 1, 2018, or 12 months after FERC approval.

Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry
Dislikes 0	

Response

Christy Koncz - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG

Answer	No
Document Name	

Comment

PSEG agrees with and supports EEI's comments.

Likes 1	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Recommend September 1, 2019 because of budget cycles and configuration changes impacting implementation provisions for early adoption of version 7 to align with version 6's enforcement.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

The requirements for LIBCS are in flux, for example, the Standards Drafting team is also adding requirements related to transient cyber assets for LIBCS. Implementing requirements on low impact assets is particularly burdensome due to the sheer numbers of assets, e.g., some of our members have thousands of assets with low impact BCS. Nation-wide there are approximately 55,000 substations, each will require owner/operator visits to make the adjustments. Even minor adjustments to the requirements such the LERC definition changes and adding any new requirements, will require a significant undertaking by the industry. Although we appreciate that NERC and the SDT is trying to rapidly implement these requirements to be responsive to FERC, we caution NERC and FERC to consider potential impacts to the Reliability of the bulk electric system and seek methods to minimize these impacts.

Many of our members have already begun to implement the CIP-003-6 LIBCS requirements and all of our members will have started by January 2017 to be able to make the CIP-003-6 September 2018 effective date. The CIP-003-7 and LERC modifications are due to FERC on April 1, 2017. If FERC takes 3 months to issue a NOPR, 45 days for comments, and 3 months to issue a final rule around November 15, 2017, then companies will have already significantly implemented the CIP-003-6 R2, Attachment 1, Sections 2 and 3. They will then have 10 months to switch from the CIP-003-6 to CIP-003-7 requirements. This produces unnecessary, duplicative implementation requirements for the sake of compliance (adding little to no value to security) and creates regulatory uncertainty for our members in the event regulatory obligations change, creating even more implementation challenges and burdens.

To address these implementation challenges which were caused by FERC approving CIP-003-6 and ordering modifications at the same time, we encourage the SDT to develop a CIP-003-7 approach that enables members who are already implementing CIP-003-6 to continue to do so and remain compliant with CIP-003-7 once FERC approves the new language. We believe our proposed alternative text for question 3 will alleviate this concern.

Another option would be for FERC to stop implementation of CIP-003-6, Sections 2 and 3 until FERC approves the modification, but we do not believe this is under the control of NERC or the SDT.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Response

Oliver Burke - Entergy - Entergy Services, Inc. - 1

Answer	No
Document Name	

Comment

I support comments provided by Entergy's Julie Hall.

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6

Answer	No
Document Name	

Comment

Given the proposed implementation plan, governmental authorities will have until November 31st, 2017 to fully approve the proposed revisions without extending the current September 1, 2018 deadline for CIP-003-6 Electronic Access Controls for low impact BCS. The proposed revisions allow entities more flexibility to implement electronic access controls to allow only the required access, which may result in a different solution than the type required under CIP-003-6. The November 31st, 2017 approval date would most likely be past most entities (especially larger entities) design, proposal, and purchasing stages and may result in entities not having the ability to implement the most cost efficient solution. It is requested that the implementation date be rescheduled to be " the later of September 1, 2018 or the first day of the first calendar quarter that is fifteen (15) calendar months after the effective date of the applicable governmental authority's order approving the standard". This would not explicitly extend the deadline immediately for CIP-003-7, but would reduce the timeline of uncertainty for Responsible Entities such that they would have adequate time to consider cost effective solutions.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
The requirements for low impact BES Systems are currently in flux and entities will not have certainty regarding low impact requirements until they are approved by the Commission. In addition, the sheer number of assets containing low impact BES Cyber Systems is substantial. It is going to take entities time to implement proper physical and electronic controls at all the various locations. Even minor adjustments to the low impact requirements or LERC definition will require a significant undertaking. CenterPoint Energy believes it is reasonable to request additional time to implement the requirements given that the facilities are low risk to the reliability of the BES. CenterPoint Energy recommends the effective date for CIP-003-7 R2 Attachment 1, Section 2 through 3 to be delayed two years after FERC approval.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
The proposed revisions to the Low Impact External Routable Connectivity (LERC) definition, retirement of the Low Impact Electronic Access Point (LEAP) and associated changes to the requirements for CIP-003 Attachment 1 Section 2 and 3 represent a significant shift from the currently FERC-approved definitions and requirements. The proposed changes include identifying LERC to non-BES Cyber Assets increasing the scope. Entities are well into their implementation of the approved definitions and requirements. This fundamental shift creates regulatory uncertainty for entities and timing concerns to meet the proposed implementation schedule due to re-work and the volume of assets containing low impact BES Cyber Systems. At best, FERC approval is not likely till near the end of 2017, which will be too late for most entities' budgeting schedules for work to be completed in 2018 if the revised requirements require budget changes. It's not logical to vote yes on the non-binding poll until the requirement language is closer. At a bare minimum, the 9 calendar month minimum implementation time should be increased to 24 months in case entities need to revise or significantly expand their programs.	
Likes 0	
Dislikes 0	
Response	
Robert Tallman - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name LG&E and KU Energy	
Answer	No
Document Name	

Comment
LG&E/KU supports EEI's comments. It is very challenging and resource intensive to meet one standard and then have a major component of that standard (e.g., the LERC definition) change. This requires additional expenditure of time and money to meet the new standard. There is the potential that V6 would be effective on 9/1/2018 and industry would then have to meet the V7 changes by 1/1/2019. This timing would be problematic. LG&E/KU recommends that, if approved, the V6 effective date be moved forward to the V7 date, similar to the move of V5 from 4/1/16 to 7/1/16. Additionally, this change combined with changes for TCA at Low are making the attachment to CIP-003 a requirement within itself. LG&E/KU suggests removing this from CIP-003 and creating a new standard (CIP-012) with its own implementation date that addresses all the Low requirements.

Likes 0	
Dislikes 0	

Response

Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment
SCE agrees with and supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison

Answer	No
Document Name	

Comment
Recommend September 1, 2019 because of budget cycles and configuration changes impacting implementation provisions for early adoption of version 7 to align with version 6's enforcement.

Likes 1	New York State Reliability Council, 10, ADAMSON ALAN
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
See question 1 comment.	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
Given the fundamental issues in the current draft, significant confusion by entities is likely to occur. Prior to supporting the implementation, these issues need to be addressed.	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5	
Answer	No
Document Name	
Comment	
We suggest that Version 7 be implemented instead of the effected requirements in Version 6 in order to prevent confusion and an unnecessary expenditure of resources.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
ALAN ADAMSON - New York State Reliability Council - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

AZPS is in agreement with the current Implementation Plan timeline as proposed provided that the significant scope increase about which it raised concerns in its earlier comments does not result. AZPS notes that should a significant scope increase as mentioned in the response to Question No. 1, implementation under the proposed implementation plan would be unnecessarily challenging.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	Yes
Document Name	

Comment

Although the implementation period may be reasonable, Texas Re requests the SDT provide a justification of the proposed implementation window. This is particularly important given that the proposed changes serve solely to clarify existing compliance obligations regarding the identification and development of access controls for low impact BES Cyber Assets.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Burns & McDonnell - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	Yes
Document Name	

Comment

No comment

Likes 0	
Dislikes 0	

Response

David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC

Answer	Yes
Document Name	

Comment

No Comments	
Likes 0	
Dislikes 0	
Response	
Yvonne McMackin - Public Utility District No. 2 of Grant County, Washington - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michiko Sell - Public Utility District No. 2 of Grant County, Washington - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - NA - Not Applicable - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey Watkins - Jeffrey Watkins On Behalf of: Eric Schwarzrock, Berkshire Hathaway - NV Energy, 5; - Jeffrey Watkins	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Emily Rousseau - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO-NERC Standards Review Forum (NSRF)	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 1, 5, 3; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Varnell - Tenaska, Inc. - Tenaska Power Services Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mary Cooper - Alameda Municipal Power - 3,4 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Dufresne - Hydro-Qu?bec Production - 5	
Answer	
Document Name	
Comment	
We support the comments of TransÉnergie.	

Likes 0	
Dislikes 0	
Response	
Julie Ross - Austin Energy - 3	
Answer	
Document Name	
Comment	
I support Andrew Gallo's comments.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF	
Answer	
Document Name	
Comment	
WEC Energy Group (including Wisconsin Electric and Wiscsonsin Publice Service).participated in the development of and support EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	
Document Name	
Comment	
signing on with NIPSCO comments of Sarah Gasienica	
Likes 0	
Dislikes 0	

Response

7. If you have additional comments on the proposed revisions to address the FERC directive regarding the LERC definition that you have not provided in response to the questions above, please provide them here.

John Varnell - Tenaska, Inc. - Tenaska Power Services Co. - 6

Answer	
Document Name	

Comment

FERC Order 822 wanted mor information on the term “direct” not through it out,

Likes 0	
Dislikes 0	

Response

David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC

Answer	
Document Name	

Comment

The comments expressed herein represent a consensus of the views of

members of the SERC Critical Infrastructure Protection Committee only and should not be construed as the

position of SERC Reliability Corporation, its board, or its officers.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	
Document Name	

Comment

AE believes the SDT should define “asset.” Based on the “Low Impact” criteria in CIP-002, we believe the SDT should define the term “Asset” as follows:

-- Control Centers and backup Control Centers

-- Transmission stations and substations

-- Generation resources

-- Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements

-- Special Protection Systems that support the reliable operation of the Bulk Electric System

-- For Distribution Providers, Protection Systems specified in Applicability Section 4.2.1 of CIP-002.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	
Document Name	

Comment

From a formatting perspective it would be helpful to use a consistent approach to paragraph and section numbering. There is a mixture of numbers, bullets, and no numbering at all. A consistent number format is very helpful when trying to reference parts or sections of the document in attachments 1 & 2. We suggest you use the same format as is used in the main standard body.

Likes 0	
Dislikes 0	

Response

Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6

Answer	
Document Name	

Comment

signing on with NIPSCO comments of Sarah Gasienica

Likes 0	
Dislikes 0	

Response

Emily Rousseau - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO-NERC Standards Review Forum (NSRF)

Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	
Document Name	
Comment	
Regarding non-binding VRF/VSL poll, it is inconsistent with the risk based methodology for an entity that updates it's high and medium impact cyber security policy after 15 months but prior to 16 months to have a lower VSL, but the same entity that fails to update the low impact cyber security policy in 15-16 months to have a medium VSL.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF	
Answer	
Document Name	
Comment	
WEC Energy Group (including Wisconsin Electric and Wiscsonsin Publice Service).participated in the development of and support EEI's comments.	
Likes 0	
Dislikes 0	
Response	

Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	
Document Name	
Comment	
ITC Holdings requests that NERC place items related to electronic boundary protection in CIP-005, not CIP-003. The same should apply to physical protections of low. Low requirements should be placed in the standard that closely matches the medium requirements. Transient devices should be in their own standard (i.e., CIP-012). The CIP-003 standard should not be a parking lot for newly developed requirements.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	
See question 1 comment.	
Likes 0	
Dislikes 0	
Response	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	
Document Name	
Comment	
Transient LERC(s) should be addressed in this Standard or in response to the FERC directive to address Transient Cyber Assets at Low Impact. The Standard should address dynamic connectivity into low impact substations. This may include Transient Cyber Assets, mobile substations, intermittent session based communication, and cellular network connections.	
Likes 0	
Dislikes 0	
Response	

Patrick Farrell - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
Due to the several comments and issues raised regarding the LIBCS, the SDT may consider separating Low Impact BES Cyber Systems from CIP-003, and instead create a new standard, or revise CIP-002-5.1, to include LIBCS specific requirements.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Burns & McDonnell - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	
Document Name	
Comment	
Burns & McDonnell has noticed many comments regarding the “asset boundary” part of the proposed definition is causing some concern with Registered Entities (Entity), with most of those comments related to what is the boundary and could there be differences of opinion on what is the boundary at audit time between the Entity and Audit Teams. We feel the information in the Guidance and Technical Basis (GTB) section of proposed CIP-003-7 has sufficient information to indicate what could be the “asset boundary” and using a practical approach in determining the boundary there should be no question as long as the Entity clearly documents how they arrived at the identification of the boundary. We feel it would be beneficial if the GTB text provided some guidance on how the boundary could be documented to reduce concerns that their determination of the boundary would be questioned by Audit Teams.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	
Comment	
These standards are still ambiguous and would therefore be subjective to the auditor.	
Likes 0	

Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
The current effective date of CIP-003 R1.2.3 requiring a Cyber Security Plan for “Electronic access controls for Low Impact External Routable Connectivity (LERC) and Dial-Up Connectivity” is April 1, 2017. CenterPoint Energy believes that the Cyber Security Plans for Low Impact BCS in R1.2.3 is dependent upon the definition of LERC and the requirements for CIP-003, Attachment 1, Section 2 and 3 that are currently in flux. CenterPoint Energy recommends that the effective date for CIP-003 R1.2 to align with the effective dates for CIP-003-7, Attachment 1, Section 2 and Section 3. With the ongoing modifications to the low impact BES Cyber Systems requirements, the SDT should consider removing the low impact BES Cyber Systems requirements from CIP-003 and creating a new standard.	
Likes 0	
Dislikes 0	
Response	
Julie Ross - Austin Energy - 3	
Answer	
Document Name	
Comment	
I support Andrew Gallo's comments.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE suggests that “routable protocol(s)” and/or “routable communication(s)” should be defined in the NERC Glossary of Terms and examples given within the definition.

Texas RE ultimately believes that low impact BCAs should be within an Electronic Security Perimeter (ESP). Texas RE would like to reference the purpose statement in CIP-005-5, which reads, “*To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES*.”

Although not directly within the scope of this project, Texas RE encourages the drafting team to review the Violation Time Horizons set forth in the Standard. From an Enforcement perspective, Violation Time Horizons have a significant impact on the ultimate penalty determination. As such, the SDT may wish to consider the current Operations Planning time horizon set forth in the Standard and articulate a basis for this conclusion.

Likes 0	
Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10

Answer	
Document Name	

Comment

The SPP RE respectfully offers the following two comments: (1) The SPP RE believes there is a significant gap in the revised requirements and accompanying definition of Low Impact External Routable Communication (LERC). Unlike the requirements for High and Medium Impact BES Cyber Systems, there is no concept of a Protected Cyber Asset due to the absence of an Electronic Security Perimeter. While the requirement for electronic access controls would conceivably protect non-BES Cyber Assets connected to the same routable network, there is no requirement to protect such Cyber Assets from unauthorized physical access. The requirement is to control physical access, based on need as determined by the Responsible Entity, to the asset or the locations of the low impact BES Cyber Systems within the asset. To the extent that non-BES Cyber Assets are collocated with Low Impact BES Cyber Systems, physical protections will be afforded. However, with the provision in the “Determining Asset Boundary” section of the Guidelines and Technical Basis to expand the “asset boundary” beyond the “fence line,” coupled with the option to control physical access only to the locations of the Low Impact BES Cyber Systems as opposed to protecting the asset in total, non-BES Cyber Assets could reside within the defined asset boundary but not within the physical protection zones permitted by the Standard. This gap introduces an unacceptable risk of attack that would allow the malicious actor ready access to the unprotected Cyber Assets and thus to the connected network, bypassing the electronic access controls designed to protect the Low Impact BES Cyber Systems. (2) The SPP RE has repeatedly encountered the argument that data traffic passed over Layer 2 networks is not routable communication. There is a significant difference between routable communications and routing networks. Layer 3 (routable) traffic encapsulated with Layer 2 headers for transmission over a Layer 2 network segment does not result in non-routable communications. It is the presence of network (not MAC) addresses in the Layer 3 header of the data packet that makes the communication routable. This should be clarified in the Guidelines and Technical Basis section of CIP-003-7, or the term should become a defined term in the NERC Glossary.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
EEI greatly appreciates the work of the Standards Drafting Team and the NERC staff. In additon to our comments submitted under the other questions, we offer the following additional comment. Given our concerns regarding the ongoing modification to the LIBCS requirements, the SDT may want to consider removing the low impact requirements from CIP-003 and create a new standard.	
Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no NextEra	
Answer	
Document Name	
Comment	
Transient LERC(s) should be addressed in this Standard or in response to the FERC directive to address Transient Cyber Assets at Low Impact. From a formatting perspective it would be helpful to use a consistent approach to paragraph and section numbering. There is a mixture of numbers, bullets, and no numbering at all. A consistent number format is very helpful when trying to reference parts or sections of the document in attachments 1 & 2. We suggest you use the same format as is used in the main standard body. The Standard should address dynamic connectivity into low impact substations. This may include Transient Cyber Assets, mobile substations, intermittent session based communication, and cellular network connections.	
Likes 0	
Dislikes 0	
Response	
Christy Koncz - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG	
Answer	
Document Name	
Comment	

PSEG agrees with and supports EEI's comments.

Likes 1	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	
Document Name	

Comment

CIP-002 should be split into two separate standards. R1, R1.1, and R1.2 are planning functions and require a great deal of hair splitting because the deliverable is not clearly defined in the standard. R1.3 and the rest of the standard is about cyber security. Planning engineers don't typicall know cyber security and cyber security people don't typically know transmission systems. No one wants to take responsibility for a standard and analysis that they have no other need to know. Rewriting the standard to separate R1, R1.1, & R1.2 from R1.3 and R2 would streamline the compliance effort tremendously.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	
Document Name	

Comment

CIP-002 should be split into two separate standards. R1, R1.1, and R1.2 are planning functions and require a great deal of hair splitting because the deliverable is not clearly defined in the standard. R1.3 and the rest of the standard is about cyber security. Planning engineers don't typicall know cyber security and cyber security people don't typically know transmission systems. No one wants to take responsibility for a standard and analysis that they have no other need to know. Rewriting the standard to separate R1, R1.1, & R1.2 from R1.3 and R2 would streamline the compliance effort tremendously.

Likes 0	
Dislikes 0	

Response

Roger Dufresne - Hydro-Qu?bec Production - 5

Answer	
Document Name	
Comment	
We support the comments of TransÉnergie.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	
Document Name	
Comment	
The proposed solution to address the FERC directive must allow entities to leverage and extend work already completed to meet the currently approved CIP version 6 requirements as work continues to comply with the revised requirements solution for CIP version 7. The implementation plan must allow adequate time to complete the CIP version 7 changes taking into consideration the large volume of lows.	
Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	
Document Name	
Comment	
Hydro One supports comments submitted by NPCC RSC.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	

Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	
Document Name	
Comment	
Thank you to the SDT for all of your hard work and dedication.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	
Document Name	
Comment	
Kansas City Power and Light Company endorse the comments offered by Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	
Document Name	

Comment
(1) We are concerned the Implementation Plan makes no mention of current efforts to address LEAPs. What guidance is available for documenting and testing LEAPs? How will Regional Entities conduct audits during the period identified within the Implementation Plan? What actions should Registered Entities follow during this period? (2) We believe the SDT should remove the Interchange Coordinator and Interchange Authority functions from the list of applicable functional entities, as these functions were retired in 2015. (3) We thank you for this opportunity to comment.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	
Document Name	

Comment
In regards to the non-binding VRF/VSL poll, NRECA would like to point out an inconsistent use of the VSLs. As currently drafted, updates to a high or medium impact cyber security policy after 15 months, but prior to 16 months is assigned a low VSL, but the same entity that fails to update its low impact cyber security policy in the same timeframe is assigned a medium VSL. This is not consistent with NERC's risk-based focus on standard development and should be revised to assign a low VSL for the failure to update it low impact cyber security policy during the same timeframe. NRECA appreciates the time and effort of the SDT.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3	
Answer	
Document Name	

Comment

Cowlitz PUD commends the work by the SDT, and supports the general direction being taken.

Likes 0	
Dislikes 0	

Response

Matt Stryker - Matt Stryker On Behalf of: Jason Snodgrass, Georgia Transmission Corporation, 1; - Matt Stryker

Answer	
Document Name	

Comment

Please note, we are in full agreement and support of comments submitted by the NRECA. In addition, we have several concerns regarding communications that pass through an asset boundary. We are concerned that communications will pass through the asset boundary but will not terminate on anything inisde the boundary (i.e. fiber cable passing through). We are also concerned about identifying asset boundaries for shared facilities because we are under the impression that both entities have to account for all coummunications. In the event that one of the entities' is not a NERC registered entity, we are conerned that we would need to account for all communication paths including those that have nothing to do with the BES. We recommend limiting the scope only to those paths that are used for BES communications or connect to BES Cyber Assets.

Likes 0	
Dislikes 0	

Response

Oshani Pathirane - Oshani Pathirane On Behalf of: Paul Malozewski, Hydro One Networks, Inc., 1, 3; - Oshani Pathirane

Answer	
Document Name	

Comment

Hydro One Networks Inc. supports the NPCC RSC's comments on this question in its entirety.

Likes 0	
Dislikes 0	

Response

Johnny Anderson - IDACORP - Idaho Power Company - 1

Answer	
Document Name	

Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
John Bee - Exelon - 3	
Answer	
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Ruth Miller - Exelon - 5	
Answer	
Document Name	
Comment	
See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Exelon - 6	
Answer	
Document Name	
Comment	

See Exelon TO Response	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	
Document Name	
Comment	
NRG supports the comments submitted by NPCC (Ruida Shu on 9/6/16): Transient LERC(s) should be addressed in this Standard or in response to the FERC directive to address Transient Cyber Assets at Low Impact. From a formatting perspective it would be helpful to use a consistent approach to paragraph and section numbering. There is a mixture of numbers, bullets, and no numbering at all. A consistent number format is very helpful when trying to reference parts or sections of the document in attachments 1 & 2. We suggest you use the same format as is used in the main standard body. The Standard should address dynamic connectivity into low impact substations. This may include Transient Cyber Assets, mobile substations, intermittent session based communication, and cellular network connections.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
From FERC Order 822 paragraph 73: “The Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term “direct” as it is used in the proposed definition.” BPA believes the proposed changes to LERC expand the amount of items included, and do not directly address the ambiguity of the term “direct”, as directed by the Commission.	

The decision to do away with LEAP, though understandable from an economic standpoint, would have profound implications on access control implementation and enforcement.

Expansion of scope is counterproductive to the protection of the BES cyber assets.

BPA proposes that the SDT retain LEAP and address the Commission's instruction to "provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition."

Likes 0	
Dislikes 0	

Response

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy

Answer	
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment

PacifiCorp supports comments submitted by Edison Electric Institute. Also, while PacifiCorp understands the justification provided for the approach the SDT took, PacifiCorp believes that the approach adds an increased compliance burden without added benefit to the security of BES, or any assurance that entities will not be asked for a list of BES Cyber Assets at Low Impact BES Assets.

Likes 0	
Dislikes 0	

Response

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray

Answer	

Document Name	
Comment	
In general, focus on protection of control communications versus non-critical communications. Also, some of the Reference Models may be incorrect in the labelling of non-routable versus routable protocols (e.g. Reference Model 1 left-hand side).	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	
Comment	
PacifiCorp supports comments submitted by Edison Electric Institute. Also, while PacifiCorp understands the justification provided for the approach the SDT took, PacifiCorp believes that the approach adds an increased compliance burden without added benefit to the security of BES, or any assurance that entities will not be asked for a list of BES Cyber Assets at Low Impact BES Assets	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	
Comment	
: PacifiCorp supports comments submitted by Edison Electric Institute. Also, the language in the definitions and CIP-003-7 currently out for vote is a substantial rewrite of the requirements as approved by FERC. PacifiCorp cannot afford to wait to begin implementation until a revised standard is approved by FERC, meaning that any approved version that does not allow PacifiCorp to leverage work efforts already completed in alignment with the current FERC approved standard would lead to duplicative effort and costs. Any attempt to compress the overall timeline for implementation could results in a negative impact to the reliability of the bulk electric system.	
Likes 0	
Dislikes 0	
Response	

Additional comments received from John Babik of JEA

1. Definition: The SDT replaced the term *Low Impact External Routable Connectivity* with *Low Impact External Routable Communication (LERC)* and revised the definition such that it is relevant to the type of communication that occurs crossing the boundary of the BES asset that contains the low impact BES Cyber Systems. This more clearly aligns with the output of CIP-002-5.1 Requirement R1, Part 1.3. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

Yes:

No: NO

Comments: Low Impact External Routable Communication (LERC) – A routable protocol communication that crosses the boundary of an asset containing one or more low impact BES Cyber Systems, excluding communications between intelligent electronic devices used for time-sensitive protection or control functions between non-Control Center BES assets containing low impact BES Cyber Systems including, but not limited to, IEC 61850 GOOSE or vendor proprietary protocols.

NERC SDT has stated that in this revision, the term Low Impact External Routable Connectivity has been changed to Low Impact External Routable Communication (LERC) and simplified so that it is an attribute of a BES asset concerning whether there is routable protocol communications across the asset boundary without regard to 'direct vs. indirect' access that may occur.

However the new definition add to further confusion as it has added the term “crosses the boundary of the asset”. This terminology will require that even BES assets where no routable communication to BES cyber asset, direct or indirect exists, entity will be required to provide evidence to demonstrate the negative, that means absence of communication path to the BES cyber asset. Rather than reviewing the the BES Cyber Asset/System connectivity, it will the obligated to review connectivity across the asset as prove that the BES connectivity is restricted. There are significantly high quantity of BES Cyber Assets with Low BES Cyber asset, and this definition will put considerable burden on the entity to prove the its compliance obligation.

It will be highly recommended that the definition should be revised to limit application to BES Cyber Assets where Low BES Cyber Assets utilizes routable communication , direct or indirect, to communicate with other Non-BES cyber assets within the BES asset or outside the BES Asset.

Additional comments received from Ruben Robles of Salt River Project

1. No

SRP sees the “…boundary of an asset…” as an arbitrary concept. The Guidance and Technical Basis does not provide a framework to determine the “asset boundary.” It simply provides examples of what an asset boundary may be. SRP appreciates that the SDT provided the flexibility by allowing the Responsible Entity to define the BES asset boundary. However, more clarification is needed. It is unreasonable to create controls, policies, processes, and procedures around a concept that relies on an arbitrary idea. Additionally, if the asset boundary is meant to be defined by the Responsible Entity, then it should also be a NERC defined term with so much hinging on that concept.

The term “intelligent electronic devices” is ambiguous. There are many definitions of what is thought to be an intelligent electronic device. It would seem best to use the term Cyber Asset if that is what is meant so as to avoid ambiguity.

SRP agrees with Seattle City Light. SRP also has a network for non-operational devices such as printers and desktops at assets “…containing one or more low impact BES Cyber System(s)” that cross the boundary of the asset. The new definition does not explicitly exclude those networks. As the LERC definition reads, if an asset has at least one BES Cyber System, then all routable protocol communication that crosses the boundary of the asset, with said BES Cyber System, is in scope. SRP does not believe this was the intent of the SDT and would ask the SDT to edit the suggested definition revision to reflect the true intent.

LERC brings more devices into scope at the lows than the BCA concept does at the mediums. An example of this at SRP is that there may be a transformer bushing monitor at a medium that is not in the ESP and does not impact the BES in order to result as a BCA. Therefore, the transformer monitor is not burdened by all of the efforts for compliance. However, at a low site, the transformer monitor would be brought into scope as requiring evidence of compliance and the processes to create and maintain that evidence. The same can be stated for dissolved gas monitors, temperature monitors, weather stations, and the many other devices that have no impact on the BES at all. This creates an unnecessary burden and cost simply for compliance.

2. Yes

SRP agrees with removing the term and appreciates the SDT for providing clearer wording.

3. Yes

SRP agrees with the revision and appreciates the SDT for clarifying “inbound and outbound bi-directional routable protocol access” as simply electronic access. SRP further appreciates the SDT for providing example controls in attachment 2. However, SRP also agrees with the comment made by Dominion Resources, Inc., and would appreciate clarification of the referenced verbiage in Model 7.

4. Yes

No comments

5. No

SRP echoes the comments made by Seattle City Light and would appreciate a model diagram clearly indicating a network used purely for non-operational traffic as out of scope for LERC. Additionally, SRP is requesting a model diagram explaining LERC for technologies such as Multiprotocol Label Switching (MPLS) or Carrier Ethernet used for Communication Networks

SRP also agrees with the comment made by Independent Electricity System Operator and identified many uses of “LEAP” shown in graphics. SRP is assuming this to be an oversight and understands the SDT will remove any reference to the term “LEAP.”

SRP also finds it confusing that the SDT uses the term “BES assets” in the Guidance and Technical Basis as well as the Standard Development Timeline. This term is defined on page 1 of the Guidance and Technical Basis as “any assets containing low impact BES Cyber Systems”. SRP suggests that the SDT not create informally defined terms when describing impacted assets.

6. No

9 months does not allow adequate time for the budgeting process or procurement of the infrastructure needed in addition to the planning and coordination of the installation of new architecture required to support the standard. Additionally the peak loads in the summer months do not support the ability to install new infrastructure between May through August.

CIP-003-6 was approved by FERC on Docket No. RM15-14-000 on 1/21/2016. The compliance date for CIP-003 Attachment 1, Sections 2 and 3 was set for September 1, 2018 per the Implementation Plan for CIP 5 Revisions, dated January 23, 2015. This means Responsible entities were provided 32 months in order to execute what was needed for compliance under CIP-003-6. In order to avoid duplicate or unnecessary effort and expense, implementation would not begin until the approval of CIP-003-7. The revised implementation plan is now only providing 9 months after approval of CIP-003-7 to implement.

SRP is requesting the same 32 months for implementation of CIP-003-7 that was afforded prior. This would set the effective date at August 1, 2020 or the first day of the first calendar quarter that is thirty-two (32) calendar months after the effective date of the applicable governmental authority's order approving the standard and NERC Glossary term, or as otherwise provided for by the applicable governmental authority.

7. SRP agrees with the comment made by Austin Energy stating "asset" should be a NERC defined term. SRP appreciates that the SDT attempted to do so in the Guidance and Technical Basis. However, if the term is being used to specifically reference something that is called out in the standards and requires controls, then it should be formally defined.