Comment Report

Project Name: 2016-02 Modifications to CIP Standards | CIP-003-TCA

Comment Period Start Date: 11/1/2016

Comment Period End Date: 11/18/2016

Associated Ballots:

There were 35 sets of responses, including comments from approximately 35 different people from approximately 35 companies representing 8 of the Industry Segments as shown in the table on the following pages.

Questions

1. If this were a formal posting, would your entity vote to approve the TCA definition, requirement language, and implementation plan as written?

2. Definition: The SDT revised the definition of Transient Cyber Asset (TCA) such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

3. Requirement R2: The SDT revised CIP-003-TCA, Attachment 1, adding Section 5 Transient Cyber Assets and Removable Media Malicious Code Mitigation Plan(s) to reflect the mandatory requirement for the Responsible Entity to develop and implement security plans to provide higher assurance against the propagation of malware from transient devices. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

4. Attachment 2: The SDT revised the measures language of CIP-003-TCA, Attachment 2, Section 5 to make the evidential language consistent with the 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 examples of temporarily connected devices, and strategies to consider in developing the Transient Cyber Asset and Removable Media malicious code mitigation plan(s) 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) date for the requirements in Section 5 of Attachment 1 in CIP-003-TCA, which will be the later of September 1, 2018 or the first day of the first calendar quarter that is twelve (12) 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 you agree with the proposed implementation time period, please note the actions you will undertake that necessitate this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

7. If you have additional comments on the proposed revisions to address the FERC directive regarding TCAs for low impact BES Cyber Systems 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
ACES Power Marketing	Ben Engelby	6		ACES Standards Collaborators - CIP	Mike Brytowski	Great River Energy	1,3,5,6	MRO
					Ginger Mercier	Prairie Power, Inc.	3	SERC
					Tara Lightner	Sunflower Electric Power Corporation	1	SPP RE
					Shari Heino	Brazos Electric Power Cooperative, Inc.	1,5	Texas RE
					Bill Watson	Old Dominion Electric Cooperative	3,4	RF
					Cassie Williams	Golden Spread Electric Cooperative	3,5	SPP RE
					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
					Ryan Strom	Buckeye Power, Inc.	3,4,5	RF
					Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	RF
					Eric Jensen	Arizona Electric Power Cooperative, Inc.	1	WECC
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Greg Froehling	Rayburn Country Electric Cooperative, Inc.	3	SPP RE

					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Carl Behnke	Southern Maryland Electric Cooperative	3	RF
					Susan Sosbe	Wabash Valley Power Association	3	SERC
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
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
Con Ed - Consolidated Edison Co. of New York	Dermot Smyth	3,4,5,6	NPCC	Con Edison	Dermot Smyth	Con Edison Company of New York	1,3,5,6	NPCC
					Edward Bedder	Orange & Rockland		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 and Energy Marketing	6	SERC

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	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
					MIchael Forte	Con Edison	1	NPCC

					Quintin Lee	Eversource Energy	1	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
					Kathleen Goodman	ISO-NE	2	NPCC
					Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
					Sean Bodkin	Dominion	4	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
Midwest Reliability Organization	Russel Mountjoy	10		MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Chuck Lawrence	American Transmission Company	1	MRO
					Chuck Wicklund	Otter Tail Power Company	1,5	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administratino	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Shannon Weaver	Midcontinent Independent System Operator	2	MRO
					Brad Parret	Minnesota Power	1,5	MRO

					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service	3,5,6	MRO
					Tony Eddleman	Nebraska Public Power District	1,3,5	MRO
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Tony Eddleman	Nebraska Public Power District	1,3,5	MRO
					Steve Keller	Southwest Power Pool Inc	2	SPP RE
Midcontinent ISO, Inc.	Terry Bllke	2		IRC-SRC	Christina Bigelow	ERCOT	2	Texas RE
					Kathleen Goodman	ISONE	2	NPCC
					Ben Li	IESO	2	NPCC
					Terry Bilke	MISO	2	RF
					Greg Campoli	NYISO	2	NPCC
					Mark Holman	PJM	2	RF
					Charles Yeung	SPP	2	SPP RE
Oxy - Occidental Chemical	Venona Greaff	7		Oxy	Venona Greaff	Occidental Chemical Corporation	7	SERC
					Michelle D'Antuono	Ingleside Cogeneration LP.	5	Texas RE

1. If this were a formal posting, would your entity vote to approve the TCA definition, requirement language, and implementation plan as written?

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
See question 3 comments for our explaination.	
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 suggest the drafting team include the approval of the RSAW into the Implementation Plan as this is a significant and related document. Also, we have a concern pertaining to the background information in the Implementation Plan (page 1) in reference to the terms “Low Impact BES Cyber Systems” and Low Impact Control Centers.” The FERC Order 822 language mentions both terms, and both are capitalized; however, nether term is defined in the NERC Glossary of Terms. Additionally, in the Standard, the lower case term “low impact BES Cyber Systems” is used throughout the document. If these terms are defined in a particular Standard, we suggest adding these terms to the Glossary of Terms; if not, confusion and the appearance of inconsistency in the Standard Development Process may result. Additionally, we are concerned about tracking TCAs, and the protections surrounding the various TCAs, that are being connected to the Low Impact. From a Cyber Security perspective, utilization of the cleanest possible computers makes sense; however, from a risk perspective, low impact BES Cyber Systems are, by definition, low risk. Mandating TCAs for low impact Cyber Systems will result in additional costs to utilities without clear justification of the risk. Ultimately, the TCA requirements are more stringent than the requirements for low impact Cyber Systems. We would recommend that the utilities use their business computers to connect to the cyber system.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No

Document Name	
Comment	
We believe the SDT should consider these comments before continuing with a formal posting.	
Likes 0	
Dislikes 0	
Response	
Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP	
Answer	No
Document Name	
Comment	
We would not support the requirement language that is proposed for Transient Cyber Assets (TCA), as this revision introduces controls that are similar to controls that would be written for medium impact BES Cyber Systems. There needs to be differentiation between a low impact and medium impact requirement, as this proposal blurs the line between the two impact levels.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	No
Document Name	
Comment	
See comments below.	
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 and KU Energy’s concern with certain wording in the Guildelines and Techinal basis are addressed in the response to Question 5 below.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	No
Document Name	
Comment	
In general, this okay. Please add to Attachment 2, Section 5: “A log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset is not required.” Reason: This is parallel to and in line with the specific statement in CIP-002 and CIP-003 that “an inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.”	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
The redlines to the TCA definition do not substantively improve the TCA definition.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5 - WECC	
Answer	No
Document Name	
Comment	

The new definition does not explicitly state where it applies to Low Impact BES Cyber Systems, including Low Impact Control Centers as requested in Order No. 822. The definition should not limit the time of connection to 30 days since some diagnostic tools may be connected indefinitely.

Likes 0	
Dislikes 0	

Response

Yuguang Xiao - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 3,4,5,6 - NPCC, Group Name Con Edison

Answer	Yes
Document Name	

Comment

Change answer to NO. Con Edison is supporting NPCCs comments on this question.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Seminole supports the definition and anticipates voting yes based on current analysis. Seminole requests that the team consider whether a line should be added to the definition:

2.5: not an Electronic Access Control and Monitoring System (EACMS) with high or medium impact BES Cyber Systems;	
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 would vote to approve the revised TCA definition and the implementation plan as currently drafted. Depending on the SDT's response to our comment on Question 4, Tri-State may have concerns with the standard draft.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
no comments	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,SPP RE,RF	
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	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,3,5 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Matt Stryker - Georgia Transmission Corporation - 1 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
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	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Bilke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
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	

Linsey Ray - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hong Ablack - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. Definition: The SDT revised the definition of Transient Cyber Asset (TCA) such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

Teresa Cantwell - Lower Colorado River Authority - 1,5,6

Answer	Yes
Document Name	

Comment

no comments

Likes 0	
Dislikes 0	

Response

Hong Ablack - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	Yes
Document Name	

Comment

CenterPoint Energy supports the revised Transient Cyber Asset (TCA) definition. CenterPoint Energy recommends that the SDT also consider updating the "Removable Media" definition to align with the proposed changes to the TCA definition. CenterPoint Energy proposes the following revisions to the "Removable Media" definition to provide clarity and applicability for low, medium, and high impact BES Cyber Systems:

Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP ***containing high or medium impact BES Cyber Systems****, or a Protected Cyber Asset* ***associated with high or medium impact BES Cyber Systems****. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.*

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	Yes
Document Name	

Comment

The IRC recommends that the standard drafting team consider revising the definition of "Removable Media" so that it is consistent with the revised definition of TCA.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

The IESO recommends that the standard drafting team consider revising the definition of "Removable Media" so that it is consistent with the revised definition of TCA.

Likes 0	
Dislikes 0	

Response

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 3,4,5,6 - NPCC, Group Name Con Edison

Answer	Yes
Document Name	

Comment

Change answer to NO. Con Edison is supporting NPCCs comments on this question.

Likes 0	
Dislikes 0	

Response

Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
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	
Linsey Ray - Oncor Electric Delivery - 1 - Texas RE	
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	
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	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Matt Stryker - Georgia Transmission Corporation - 1 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 3,5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,3,5 - WECC	
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	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5 - WECC	
Answer	No
Document Name	
Comment	

The revised definition does not explicitly state applicability to Low Impact BES Cyber Systems including Low Impact Control Centers. Also, the definition should not limit the time of connection to 30 days since some diagnostic tools may be connected indefinitely.

If the SDT intended to include all low impact BES Cyber Assets as part of the definition, Reclamation recommends changing the definition in item four to the following:

4. temporarily directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) to any:

- BES Cyber Asset associated with high, medium, or low impact BES Cyber Systems
- network within an Electronic Security Perimeter containing high or medium impact BES Cyber Systems, or
- PCA associated with high or medium impact BES Cyber Systems.

Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	

- Because the redlines that NERC SDT has included use “and” statements (instead of “or” statements), NRG does not agree that the redline changes effectively address the Low Impact BCS. Any transient cyber asset requirements for Low Impact BCS will increase the cyber security requirements for the Low Impact sites. The TCA definition implies that the entity would know when a TCA is connected to a low impact BES Cyber System when that BES Cyber System may not be explicitly identified.
- NRG recommends that the NERC SDT consider rewording the redline changes to the TCA definition.

Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	No
Document Name	
Comment	
We recommends No and cannot agree on alternative language that satisfies both security and compliance needs. We are not comfortable with the way the language does not address low Impact networks.	
Likes 0	
Dislikes 0	
Response	
Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP	
Answer	No
Document Name	
Comment	
We disagree with the approach taken because it is unnecessary to introduce additional requirements prior to the effect dates of low impact requirements. We strongly recommend the SDT delay any future development on low impact standards until after the effective date has passed to allow industry and the ERO Enterprise an opportunity to assess any associated risks. The FERC directive stated that NERC should develop requirements for low impact TCA “based on the risk posed to bulk electric system reliability,” and it is very difficult to assess that risk until the requirements are enforceable.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

We recommend that the SDT modify the Removable Media definition in addition to the TCA definition. Add “containing high or medium impact BES Cyber Systems” after ESP; add” associated with high or medium impact BES Cyber Systems” after Protected Cyber Asset; and add “of Removable Media” after “Examples.”

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE does not agree the changes to the proposed definition are necessary. Adding the phrase “associated with high or medium impact BES Cyber System” is redundant as PCAs inherently apply to medium and high impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Yuguang Xiao - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

See comment for Question 1.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

The current structure is confusing.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
See question 3 comments for our explaination.	
Likes 0	
Dislikes 0	
Response	

3. Requirement R2: The SDT revised CIP-003-TCA, Attachment 1, adding Section 5 Transient Cyber Assets and Removable Media Malicious Code Mitigation Plan(s) to reflect the mandatory requirement for the Responsible Entity to develop and implement security plans to provide higher assurance against the propagation of malware from transient devices. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 3,4,5,6 - NPCC, Group Name Con Edison

Answer	Yes
Document Name	

Comment

Answer = Yes. Con Edison is supporting NPCCs comments on this question.

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

As proposed, the modifications to Section 5 “Each Responsible Entity shall implement one or more plan(s) to achieve the objective of mitigating the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media, which shall Include”. There is a concern, that if malware is introduced onto a low impact BES Cyber System from a TCA, and the malware was not prevented by the controls you implemented then this could be interpreted to be a violation The Standards Drafting Team should clarify that an introduction of malware, even when an entity has controls in place, is not a violation unless it is shown the entity did not have controls in place or the entity did not use those controls.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,3,5 - WECC

Answer	Yes
Document Name	

Comment

We would like additional clarification to help our understanding of the responsibilities of Third Pary TCA's and Removable Media Mitigation Plan(s).

Likes 0	
Dislikes 0	

Response

Matt Stryker - Georgia Transmission Corporation - 1 - SERC

Answer	Yes
Document Name	

Comment

Regarding 5.1 & 5.2: The phrase "use of one or combination of the following method," provides little direction as to the measurability of success in compliance in terms of how many methods would be acceptable.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	Yes
Document Name	

Comment

Exelon is in general agreement with the approach to mirror the CIP-010 language for TCAs associated with High and Medium BCSs in CIP-003-TCA for TCAs associated with Low BCSs. However, if a decision is made to revise both CIP-010 and CIP-003 language relevant to TCAs, we believe the following additional revisions should be also be made:

1. The Standard should remove the language requiring that the mitigation plans "achieve the objective of mitigating the introduction of malicious code." This suggests that any introduction of malicious code would be noncompliant because that would be a failure to "achieve the objective." The Standard should instead require the implementation of "one or more plan(s) to mitigate the introduction . . . ."

2. For 5.1, if any "other methods to mitigate the introduction of malicious code" are acceptable, the Standard should simply require that Responsible Entities implement "one or more methods to mitigate the introduction of malicious code." The examples and possibilities can be included in the GTB.

3. For 5.2, if any "other methods to mitigate the introduction of malicious code" are acceptable, the Standard should allow other parties managing such assets to implement "one of more methods to mitigate the introduction of malicious code." The examples and possibilities can be included in the GTB.

4. Provide more clarity on what the Standard means by "managed by a party other than the Responsible Entity." Attachment 1 Section 5 distinguishes between TCAs managed by the Responsible Entity and TCAs managed by a party other than the Responsible Entity. However, the Standard does not explain how to determine who "manages" a TCA. Given the various agency, vendor, and service provider relationships in the industry, the Standard

should provide specific guidance on how to determine whether a Responsible Entity or another party is “managing” a TCA. To confuse this further, the GTB refer to TCAs being under the “control” of the Responsible Entity or a third party.

4a. If a contractor is working on a temporary basis for a Responsible Entity, are any TCAs used by that contractor “managed” by the Responsible Entity? If the TCAs are provided by the temporary agency, does that change the analysis?

4b. If a TCA is used by a vendor providing services to the Responsible Entity, is that TCA “managed” by the vendor? What if the vendor has agreed to follow the Responsible Entity’s CIP compliance program?

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

Note that while the IESO agrees with the revisions we do not have any low impact assets which would be impacted therefore we would likley abstain from a vote.

Likes 0	
Dislikes 0	

Response

Terry Bilke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	Yes
Document Name	

Comment

Note that while the IRC members agree with the revisions we do not have any low impact assets which would be impacted therefore we would likley abstain from a vote.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	Yes
Document Name	
Comment	
See comments to question 2.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
no comments	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,SPP RE,RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
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	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Oncor Electric Delivery - 1 - Texas RE	
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	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hong Ablack - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

The proposed CIP-003, Attachment 1 additions appear to provide a workable framework for meeting FERC's directive set forth in FERC Order No. 822 that the revised Standard provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk to BES reliability. Specifically, the proposed additions to CIP-003, Attachment 1 require entities to develop "and implement one or more plans to achieve the objective of mitigating the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets (TCAs) or Removable Media." Thus, although the proposed additions to CIP-003, Attachment 1 provide registered entities with broad discretion in how to develop protections for TCAs and Removable Media, Texas RE interprets the proposed additions to CIP-003, Attachment 1 as appropriately requiring entities to: (1) develop procedures to achieve the obligation of mitigating the introduction of malicious code to low impact BES Cyber Systems; and (2) implement those procedures to achieve that objective. That is to say, the proposed additions appropriately reflect a results-based approach that provides flexibility in achieving the reliability goal, but at the same time requires the elected methods to actually work to mitigate the introduction of malicious code.

Texas RE recommends including the same criteria for low BES Cyber Assets in CIP-003 as it does for medium and high BES Cyber Assets in CIP-010. The standards will be more consistent and achieve reliability objectives. Texas RE suggests including the following language from CIP-010:

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient

Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business

functions."

"3.1. Removable Media Authorization: For each individual or group of Removable

Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group."

Texas RE recommends making the following grammatical changes to the attachment language:

- Page 26, Section 5, reads "*shall implement one or more plan(s)*", it should read "*shall implement one or more documented plan(s)*", to stay consistent with the other CIP Standard language, which requires entities to have documented plans.
- Page 26, Section 5.1, reads: "*For Transient Cyber Asset(s) managed by the Responsible Entity, if any, use of one or a combination*". The term "of" should be removed.
- Page 29, Section 5, #2 - there should be a period (.) after "…capability".

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The SDT has clearly defined Transient Cyber Asset which in essesence is a physical object that can be connected to **or** something that has the ability to transmit executable code to BES Cyber Asset, to a network within an ESP or PCA. The second part of Section 5, deals with Removable Media Malicious Code Mitigation Plan(s). Removable Media is defined as any storage device that can be removed from a computer while the system is running, i.e., CDs, USB drive, etc. The Removeable Media **is** the Transient Cyber Asset per the proposed definition. What we need to accomplish is to assure that Malicious Code is not introduced into a BES CA, ESP or PCA via a Transient Cyber Asset and be within a plan that describes how we will prevent this.

The current wording for Transient Cyber Asset and Removable Media Malicious Code Mitigation Plan(s) is confusing to entities since it has too many objectives within one sentenance. The NSRF recommends the following;

1. Section 5 should be rewritten to reflect "Transient Cyber Asset and malicious code mitigation Plan(s)".

2. Update the Rational box (or Guidelines and Technical basis) to explain that Removable Media is defined as any "storage device that can be removed from a computer while the system is running, i.e., CDs, USB drive, etc."

3. Since Removable Media is a TCA, remove "Removable Media" within the sub sections of Section 5.

If this proposition does not work for the SDT, then it is recommended the following be rewritten:

1. “Transient Cyber Asset and removable media: Malicious code mitigation Plan(s)”.

2. In order to be in line with NERC’s word defining process, either define Removable Media and Malicious Code Mitigation Plans or remove the capitalization either or both (as above).

Section 5, we do not know the difference of 5.1 and 5.3 when a TCA is removable media? This causes confusion without definitions as requested, above. Part 5.1 first bullet says the same thing as 5.3.1: to detect malicious code.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

This is too complicated and overburdensome. Our understanding is that Section 5 lays out a considerable regulatory scheme for cyber assets that are one step removed from cyber assets that are by definition low risk and unlikely to impact reliability of the BES.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Seminole appreciates the effort by the standard team to develop this draft update to CIP-003 and to provide a process consistent with those for medium and high impact Cyber Assets.

Section 4.2 of the standard specifically states:

“Facilities: …the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable…

Whereas the attachment 1 section 5.2 states:

For Transient Cyber Asset(s) managed by a party other than the Responsible Entity…

As the owner of the cyber asset not managed by the entity may also not be owned by the entity, the Transient Cyber Asset may be outside the scope of the requirement. Note this same issue is also present in the current version of CIP-010. Clarity needs to be provided regarding this issue.

There is significant ambiguity In the Guidelines and Technical Basis Section of the document related to systems with built-in protection capabilities. Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity, Seminole recommends adding the following language:

Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed <<or by documenting the built-in capabilities present and used on the Cyber Asset that prevents introduction of malicious code>>.

Seminole also recommends the use of tables such as those used in most of the other CIP standards that indicate applicability, requirement, and measure as this is a more effective method of communicating the requirement and expected evidence to the entity.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6

Answer	No
Document Name	

Comment

Dominion finds the wording in Section 5.3.2, “prior to connecting” is somewhat confusing. Similar wording in CIP-010 has been interpreted to mean that removable media must be re-checked whenever it is taken to a new BCS. In the situation where a single removable media is carried to multiple substations where each substation has one or more BCS. The removeable media is not inserted into anything other than the substation BCS. In this situation, the removable media is unlikely to become infected within the substations. Dominion recommends the SDT consider this scenario in a possible revision to the requirements to scan and mitigate prior to the initial connection to a BCS and after subsequent connections to non-BCS cyber assets capable of installing malware to the removable media. Dominion proposes the following language for Attachment 1, Section 5:

5.3 For Removable Media, prior to the initial introduction to a BCS and subsequent to connecting to any non-BCS cyber asset capable of installing malware to the removable media, and prior to connecting to a BCS perform each of the following:

5.3.1 Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigate the threat of detected malicious code on the Removable Media.

Likes 0	
Dislikes 0	

Response

Yuguang Xiao - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	

Section 5.1: The phrase "… if any,.." is not required and should be removed. It is not clear if the phrase refers to the Transient Cyber Asset or the Responsible Entity.

Section 5.2: The phrase "… if any,.." is not required and should be removed. It is not clear if the phrase refers to the Transient Cyber Asset, the Responsible Entity, or “a party other”.

Review should also include acceptance by the Responsible Entity as indicated in the examples of evidence.

The phrase ".. live operating system and software executable only" is unclear.

Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	

The phrase “ongoing or on-demand ” adds the implication Transient Cyber Asset(s) be tracked or evidence of compliance is required, which goes beyond the other requirements for assets containing low impact BES Cyber Systems, and may not be commensurate with the risk. The other two (2) controls based sections in CIP-003-7 Attachment 1 for low impact BES Cyber Systems simply require entities to have a plan and implementation based on need, with no real evidentiary audit trail requirement of performance.

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 disagree with current proposed language in Section 5.1. We assume that various members of staff will have accesss to and use of this particular asset. We suggest adding language that will help mirror the review level of the internal process (similar to section 5.2). If the assets and software are not thoroughly reviewed internally (by the Responsible Entity), the same potential issues would apply here as they would in section 5.2 (received data from external entitity).

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment
CIP-010-2 Requirement R4 includes “except under CIP Exceptional Circumstances,” we recommend that the SDT consider incorporating this exception for Transient Cyber Assets and Removable Media for low impact BES Cyber Systems as well. In Attachment 1, Section 5, the SDT can add this exception after “implement” and before “one or more plan(s)” to be consistent with the High and Medium requirements. Also, even though we realize the Section 5 language comes from the CIP-010-2 language, specifically “to achieve the objective of mitigating the introduction of malicious code”; however, this language can be improved upon by adding what the section is seeking to mitigate, i.e., the risk of the introduction of malicious code. We recommend changing the language to read “to achieve the objective of mitigating the risk of the introduction of malicious code…” Section 5.2 will have an impact on existing third party agreements (i.e., contracts), given the large number of low impact assets, renegotiating these contracts will be difficult. We recommend that the SDT consider adding forward-looking language or use of the CIP Exceptional Circumstances language to avoid requiring that entities re-negotiate contracts related to TCAs managed by other parties. Another possibility is to address this issue in the implementation plan, allowing sufficient time (e.g., 2 years from the FERC approval date) for entities to re-negotiate or modify their third party contracts.

Likes 0	
Dislikes 0	

Response

Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP

Answer	No
Document Name	

Comment

We do not support the changes to Attachment 1, Section 5. This section creates medium impact requirements for low impact systems, which is not commensurate with the risk. Smaller entities would bear an unnecessary risk of compliance by requiring medium impact controls. The purpose of creating three separate CIP impact levels was to require security controls based on risk. The low impact systems should not be required to have the same controls as the medium impact systems for TCA.

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

- It is difficult to manage the potential spaghetti effect of these standards. In the case of Low Impact BCS - You would need to have an inventory of devices that would allow plugging in a transient device (i.e. like a laptop). The proposed definition assumes that you know down to an Asset level and the definition implies that the entity would know when a TCA is connected to a low impact BES Cyber System when that BES Cyber System may not be explicitly identified.
- NRG proposes that NERC SDT place this language in the appropriate section of CIP-010.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5 - WECC

Answer	No
Document Name	

Comment

The term “Mitigation Plan(s)” may be interpreted to refer to official enforcement actions.

Reclamation recommends the following:

- Remove the term “Plan(s)” from section 5 title in Attachment 1 and not capitalize words unless they are found in the NERC Glossary of Terms. Change Section 5 title to “Transient Cyber Assets and Removable Media malicious code mitigation.”
- Change the first sentence in section 5 to “Each Responsible Entity shall implement one or more method(s) …”
- Clarify and expand Section 5.3.1 to “use of method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System (such as a development station.)”

Likes 0	
Dislikes 0	
Response	

4. Attachment 2: The SDT revised the measures language of CIP-003-TCA, Attachment 2, Section 5 to make the evidential language consistent with the requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

Teresa Cantwell - Lower Colorado River Authority - 1,5,6

Answer	Yes
Document Name	

Comment

no comments

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

The current format is hard to comprehend. Request re-formatting with bullets and numbers to separate the individual clauses.

Likes 0	
Dislikes 0	

Response

Terry Bilke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	Yes
Document Name	

Comment

Note that while the IRC members agree with the revisions we do not have any low impact assets which would be impacted therefore we would likley abstain from a vote.

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 would like to get some clarification on the language "results of scan settings for Removable Media" used in Attachment 2, Section 5.3. Our understanding is that screenshots of the scan settings/code would be enough evidence to show compliance with Section 5.3.1. Is that correct or is the intention that entities must provide the results of every scan?	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Note that while the IESO agrees with the revisions we do not have any low impact assets which would be impacted therefore we would likley abstain from a vote.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
1. 5.2’s proposed methods all presume an ability to review cybersecurity practices of third parties that those third parties may consider proprietary and not open to review.	

a. The Standard should identify examples of sufficient methods that do not require access to third-party information. For example, contracts, MOUs, and other documented understandings with third-parties requiring them to implement sufficient controls should be acceptable so long as they commit to implementing those controls.

b. If the Responsible Entity's access to that third party proprietary information is subject to confidentiality limitations that prohibit disclosure to the other entities, the Standard should explain how the Responsible Entity will be able to demonstrate compliance.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

While Seminole supports the evidence request, Seminole would like to understand the auditor approach to this requirement part.

Likes 0	
Dislikes 0	

Response

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 3,4,5,6 - NPCC, Group Name Con Edison

Answer	Yes
Document Name	

Comment

Answer = Yes. Con Edison is supporting NPCCs comments on this question.

Likes 0	
Dislikes 0	

Response

Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Hong Ablack - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
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	
Linsey Ray - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
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	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Matt Stryker - Georgia Transmission Corporation - 1 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,3,5 - WECC	

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	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	
Document Name	
Comment	
In general, this okay. Please add to Attachment 2, Section 5: “A log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset is not required.” Reason: This is parallel to and in line with the specific statement in CIP-002 and CIP-003 that “an inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.”	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE will continue reviewing facts and circumstances during compliance and enforcement reviews.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5 - WECC	
Answer	No
Document Name	
Comment	
The term “Mitigation Plan(s)” may be interpreted to refer to official enforcement actions. Reclamation recommends the following:	

- Remove the term “Plan(s)” from section 5 title in Attachment 2 and not capitalize words unless they are found in the NERC Glossary of Terms. Change Section 5 title to “Transient Cyber Assets and Removable Media malicious code mitigation.”

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

This could impact DCS upgrade or shutdowns. Requirement 5.2 is implying change control on the systems which is overly burdensome since the standards do not require an inventory on low systems.

NRG proposes that the NERC SDT place the information in Attachment 2, section 5 into bulleted format.

Likes 0	
Dislikes 0	

Response

Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP

Answer	No
Document Name	

Comment

We disagree with the proposed measures based on the same reasons we disagree with the proposed, corresponding requirements.

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

See comments above.	
Likes 0	
Dislikes 0	
Response	
Yuguang Xiao - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
In bullet 3: Suggest replacing "entity" with "the Responsible Entity or the party other than the REntity" for additional clarity and consistency with previous sections.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	No
Document Name	
Comment	
Dominion recommends that Attachement 2, Section 5, Item 3, 2nd line, the word “mitigate” should be replaced with “detect”.	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	

See above. We do support having measures that are consistent with the language used in the requirements. Further, the requirements should match the glossary of terms.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Attachment 2 Section 5 states "…or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity;". This states that a vendor will have a contract with the Responsible Entity stating what they will accomplish. The SDT should know that Responsible Entities usually only write contracts for the services that a vendor will provide. This statement needs to be rewritten stating that Responsible Entities can have a contract that covers the applicable Section 5 items, thus protecting the Responsible Entity. If non-compliance was found with the Responsible Entity, then the Responsible Entity would be able to hold the vendor in contempt of contract. Note, this will be a concern on the Supply Chain Management Standard as well.

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 examples of temporarily connected devices, and strategies to consider in developing the Transient Cyber Asset and Removable Media malicious code mitigation plan(s) 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.

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 3,4,5,6 - NPCC, Group Name Con Edison

Answer	Yes
Document Name	

Comment

Answer = Yes.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,3,5 - WECC

Answer	Yes
Document Name	

Comment

Would like more clarity on Third Party GTB language that states “to the best of their capabilities” in terms of meeting the requirements. What does this mean exactly? Reference: Requirement R2, Attachment 1, Section 5.2.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	Yes
Document Name	

Comment

See comment 1) under Question 4 above

Likes 0	

Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Note that while the IESO agrees with the revisions we do not have any low impact assets which would be impacted therefore we would likley abstain from a vote	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	Yes
Document Name	
Comment	
Note that while the IRC members agree with the revisions we do not have any low impact assets which would be impacted therefore we would likley abstain from a vote.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
no comments	
Likes 0	
Dislikes 0	

Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
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	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
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	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
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	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hong Ablack - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	
Document Name	
Comment	

The NSRF cautions the SDT that sometimes the GTB only complicates the words of the Requirements. The SDT iknows that they cannot satisfy every Registered Entity with examples in the GTB. If the GTB is needed then perhaps the Requirements are not written clearly enough.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE inquires as to why the drafting team used the new title “Supplemental Material” rather than leaving the title as “Guidelines and Technical Basis”.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

See above. We also have concerns about how the GTB are factored into Compliance and Enforcement. In some cases it appears that they create “requirements” that must be incorporated into your program this is inconsistent with prior FERC precedent. On the other hand, it is not clear whether or not you can rely on the GTB in developing your program and ensuring compliance.

Likes 0	
Dislikes 0	

Response

Matt Stryker - Georgia Transmission Corporation - 1 - SERC

Answer	No
Document Name	

Comment

The definition as proposed could result in a cyber asset unintentionally satisfying the four criteria for inclusion as a TCA.

Consider the example of a Non-BES distribution relay which is serially connected to a RTU which is a low impact BES Cyber System. If the non-BES protective relay should fail and be removed prior to the 30th consecutive calendar day after installation then it has satisfied the four parts of the definition and would be considered a Transient Cyber Asset.

The Standard Drafting Team should consider adding guidance to clarify the "intent" of a device as being a part of satisfying the definition of a TCA.

Likes 0	
Dislikes 0	

Response

Yuguang Xiao - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

Requirement 1: "… four subject matter areas …" need to be updated to "… five subject matter areas…"

Requirement 2: "… four subject matter areas …" need to be updated to "… five subject matter areas…"

Rationale for Requirement 2: "… four subject matter areas …" need to be updated to "… five subject matter areas…"

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

The information in the GTB section does not appear to be consistent with the information in Requirement R2. Our interpretation of Requirement R2 of the TCA suggests that there is not enough clarity in the Requirement to differentiate whether the focus is solely CIP-002 and its attachment 1 or if focus is the informationlocated in the document for review. We suggest adding clarity to either the Requirment or the GTB to ensure that there is no confusion as to the Requirement's intent is as well as what an audit team's interpretation of the performance of an entity during the auditing process. For example, the language used on page 45 of the Standard: "Examples of these temporarily connected devices include, but are not limited to:

Diagnostic test equipment;

Equipment used for BES Cyber System maintenance; or

Equipment used for BES Cyber System configuration.

The attachment was created to specify the capabilities and possible security methods available

to Responsible Entities based upon asset type and ownership." This detailed language from the GTB should be consistent with the Requirement language and we feel its not in this case in reference to this particular example. Additionally, the example of the devices mentioned in the GTB are not consistent with the devices in the Requirement language. We suggest that drafting team review both sections for consistency.

Likes 0	
Dislikes 0	

Response

Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP

Answer	No
Document Name	

Comment

We would like the SDT to clarify the differences between medium impact TCA and low impact TCA. We would also like the SDT to clarify in the guidelines the differences in security controls for medium and low impact BES Cyber Systems. There are no statements regarding how risks differ between levels, or how an entity should manage these risks through security controls.

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

On page 47 under the section *Requirement R2, Attachment 1, Section 5.2 – Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity,* LG&E and KU Energy believes the language quoted below appears to go beyond what FERC requires of Entities with respect to Supply Chain standard and vendor expectations, and creates a higher burden than that in the approved High and Medium TCA standard. LG&E and KU Energy suggest the wording below be removed or updated to align with FERC's expectations, and impose no higher level of compliance upon Registered Entities than that currently in place for both High and Medium TCAs.

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsibly Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code on Transient Cyber Assets it does not manage.

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

This could impact DCS upgrade or shutdowns. Attachment 2, Section 5.2 is implying change control on the systems which is overly burdensome since the standards do not require an inventory on low systems.

NRG recommends that the NERC SDT remove the change management systems reference in Examples of evidence for section 5.2.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5 - WECC

Answer	No
Document Name	

Comment

The term “Mitigation Plan(s)” may be interpreted to refer to official enforcement actions.

Reclamation recommends the following:

- Remove the term “Plan(s)” from the title “Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Mitigation Plan(s)” and not capitalize words unless they are found in the NERC Glossary of Terms. Change Section 5 title to “Transient Cyber Assets and Removable Media malicious code mitigation.”
- Add a bullet for “Equipment used for BES Cyber Asset maintenance;” in the Examples section.
- Add a bullet for “Equipment used for BES Cyber Asset configuration;” in the Examples section.

Likes 0	
Dislikes 0	

Response

6. Implementation Plan: The SDT revised the Implementation Plan such that it establishes a single effective (compliance) date for the requirements in Section 5 of Attachment 1 in CIP-003-TCA, which will be the later of September 1, 2018 or the first day of the first calendar quarter that is twelve (12) 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 you agree with the proposed implementation time period, please note the actions you will undertake that necessitate this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

Teresa Cantwell - Lower Colorado River Authority - 1,5,6

Answer	Yes
Document Name	

Comment

no comments

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Because of the state of flux of electronic access controls associated with Low Impact BES Cyber Systems, industry as a whole has not begun to fully address the electronic access control requirements for Low Impact BES Cyber Systems. Adding additional requirements to the current requirements, while the current requirements are still changing, makes it difficult for low impact only entities to begin their implementation. Rushing implementation simply to meet an earlier enforcement date does not allow for thoughtful developement of security measures. Ensuring a date that allows for a cohesive implementation between electronic access controls and TCA/Removable Media controls will provide a higher level of security than a piecemeal approach that could result from an implementation period that is too short.

Likes 0	
Dislikes 0	

Response

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 3,4,5,6 - NPCC, Group Name Con Edison

Answer	Yes
Document Name	

Comment	
Change answer to NO. Con Edison is supporting NPCCs comments on this question.	
Likes 0	
Dislikes 0	
Response	
Ryan Buss - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
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	
Linsey Ray - Oncor Electric Delivery - 1 - Texas RE	
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	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,3,5 - WECC	
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	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Bilke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	
Document Name	
Comment	
None of the changes impact the IRC members either positvely or negatively so we have no opinion on the Implimentation Plan	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not necessarily object to the SDT's proposed 12-month implementation period. However, Texas RE respectfully requests that the SDT provide a basis for its decision to adopt such a 12-month compliance window, including any data it considered in determining that this was an appropriate window for affected entities to meet their compliance obligations under the revised Standards.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
None of the changes impact the IESO either positvely or negatively so we have no opinion on the Implimentation Plan.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5 - WECC	
Answer	No
Document Name	
Comment	
Reclamation recommends a more achievable implementation plan of 24 months from the date of FERC approval.	
Likes 0	
Dislikes 0	
Response	

Hong Ablack - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
The requirements for low impact BES Cyber 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 will take entities time to implement proper controls at all the various locations. 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-TCA revisions to align with the LERC modifications.	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
NRG recommends that the NERC SDT revise the effective compliance date for the requirements in Section 5 of Attachment 1 in CIP-003-TCA to be 18 calendar months after the effective date of the applicable governmental authority's order approving the standatd and NERC Glossary term: to account for budgeting cycles.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	No
Document Name	
Comment	
Due to budget cycles and quantity of equipment that must be installed, we propose keeping the language in the "General Consideration" section but extend the interval from 12 months to 18 months.	
Likes 0	
Dislikes 0	

Response	
Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP	
Answer	No
Document Name	
Comment	
The implementation plan for TCA should not occur until 2019. We do not support the target date of September 1, 2018 because there are several other requirements that need to be met. The burden of compliance with this proposal would add significant resources and costs with implementing these low impact security measures. The implementation plan should allow for an additional budgeting cycle to ensure industry has time to implement such controls.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Although it would be helpful to implement all of the CIP-003-7 modifications at the same time, the issues we raise in the other comments should be addressed before this implementation plan is approved.	
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 suggest that the effective date be moved to eighteen (18) calendar months due to the various complexities and the scope of the process.	
Likes 0	
Dislikes 0	

Response	
Matt Stryker - Georgia Transmission Corporation - 1 - SERC	
Answer	No
Document Name	
Comment	
It is our position that there should be a focus on excellence by providing the proper timeframe for proper completion of the CIP-003 TCA requirements. The timeframe provided does not provide an adequate window for budgetary cycles, process development, implementation, and training for the successful deployment of the low impact TCA. Additional time is needed to incorporate the proper training, controls, processes and internal testing of processes to ensure success in compliance.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
Process development and implementation of Low BCS electronic access controls has been significantly delayed and remains contingent upon requirements finalization. Propose allowance of a minimum of 24 months from FERC approval date to compliance date for CIP-003-7 R2, Attachment 1 Sections 2 and 3 AND 5.	
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 disagrees with the implementation plan proposed for CIP-003-TCA, and suggests a more achievable implementation plan of 24 months from the date of FERC approval. As written, it appears that an entity will need to create an inventory of all Low BES Cyber Systems in order to ascertain whether a device that connects to a TCA is considered a “low”. It is also possible that an entity could instruct its employees/contractors to treat all devices (high, medium, or low) the same when connecting with TCA, and assume they would fall under the purview of CIP-003-TCA and perform the	

necessary work in order to maintain compliance with CIP-003-TCA. The amount of time needed for larger entities to create such an inventory, would be significant, as would the amount of time to provide training to a large number of employees/contractors in order to maintain compliance with the proposed. We do not feel that 12 months from governmental approval is an adequate amount of time to achieve compliance with the language as written currently. We recommend to the drafting team an implementation period of 24 months from FERC approval.	
Likes 0	
Dislikes 0	
Response	

7. If you have additional comments on the proposed revisions to address the FERC directive regarding TCAs for low impact BES Cyber Systems that you have not provided in response to the questions above, please provide them here.

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	
Document Name	

Comment

Please note that within the rational box for Section 5, the SDT uses “Transient devices” as did FERC in paragraph 32. Recommend that Transient device be updated to read “Transient Cyber Asset”.

Likes 0	
Dislikes 0	

Response

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 3,4,5,6 - NPCC, Group Name Con Edison

Answer	
Document Name	

Comment

None.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

Interpretation of the Attachment 1 Section 5 requirements is that evidentiary requirements are to document and implement the plan for managing malware protection for TCA and RM that are to be connected to Low BCSs, and that maintaining evidence for each instance of review and scan logs are not required.

Likes 0	
Dislikes 0	

Response

Matt Stryker - Georgia Transmission Corporation - 1 - SERC

Answer	
Document Name	

Comment

The Standard Drafting Team should consider updating the glossary definition of Removable Media to reflect similar low-impact language changes as those proposed to the definition of Transient Cyber Assets.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	
Document Name	

Comment

No additional comments

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE notes some possible issues with the proposed Violation Severity Levels associated with the proposed additions to CIP-003, Attachment 1. First, the second proposed “Lower VSL” provides that “[t]he Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to Requirement R2, Attachment 1, Section 5.3.” Although it is possible to read the VSL language as referring first to general documentation for TCAs and Removable Media and then to the two specific Removable Media elements identified in Section 5.3, this connection could be made clearer. One approach would be revise the Lower VSL to read “The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the use of method(s) to detect malicious code on

Removable Media using a Cyber Asset other than a BES Cyber System or mitigation of the threat of detected malicious code on Removable Media prior to connecting Removable Media to a low impact BES Cyber System."

Second, and related to the first issue above, the initial additional "Moderate VSL" provides that the Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3." (emphasis added). However, Section 5.3 applies to Removable Media and not TCAs. As such, the reference here seems inappropriate and potentially conflicts with the "Low VSL" for documentation of Removable Media mitigation described above. Texas RE recommends that the SDT either eliminate the reference to Section 5.3 here, or develop a new "Moderate VSL" applicable to the mitigation requirements for Removable Media in Section 5.3. The Standard Drafting Team should further ensure that this approach is consistent with the "Low VSL" for Removable Media documentation as well.

Finally, while Texas RE does not necessarily object to the general VSL assignments at this time, Texas RE respectfully requests that the SDT provide a basis for its decisions to assign VSL categories to the various elements. In particular, Texas RE would like to understand the SDT's decision to assign "Low" and "Moderate" VSL categories to Removable Media and "Moderate" and "High" VSL categories to Transient Cyber Assets.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

It would be helpful if the SDT or NERC could address what is required to demonstrate compliance with the low impact requirements at shared facilities. For example, is a Memorandum of Understanding (MOU) between the Responsible Entities that have equipment in the same low impact asset sufficient or is a Joint Registration Organization or Coordinated Functional Registration needed for the low impact CIP-003-7 requirements? If an MOU is

sufficient, what details should be addressed in the MOU? For example, which tasks or requirements is each entity responsible for performing and who is responsible for potential violations of the requirements? This is currently an unresolved issue for medium impact BES Cyber Systems and will be a bigger issue for low impact assets as there are many more low impact assets. Addressing this issue for low impact assets will also require a longer implementation timeframe given the number of low impact assets.	
Likes 0	
Dislikes 0	
Response	
Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP	
Answer	
Document Name	
Comment	
We urge the SDT to stagger its posting schedule so different drafts of the CIP standards do not have overlapping deadlines to submit comments. Industry is currently focused on implementing the existing CIP V5 standards, while also paying attention to the development of these revisions. There should not be multiple deadlines assigned to this project, as this creates a strain on CIP subject matter experts to review and provide feedback on the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	
Document Name	

Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Hong Ablack - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
CenterPoint Energy appreciates the SDT's efforts to consolidate the TCA revisions with the LERC modifications. CenterPoint Energy is in favor of filing the TCA modifications and implementation plan with the LERC modifications, if possible.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5 - WECC	
Answer	
Document Name	
Comment	
Reclamation recommends the following: • Changes associated with Transient Cyber Assets and Removeable Media should be integrated into future standards and should not be an intermin standard. • Existing NERC standard naming and numbering protocol continue to be followed and that this draft standard no longer be referred to as "-TCA."	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	

Document Name	
Comment	
no comments	
Likes 0	
Dislikes 0	
Response	