

## Consideration of Comments

<b>Project Name:</b>	2016-02 Modifications to CIP Standards   CIP-003-7(i), Implementation Plan, and definitions of TCA and Removable Media
<b>Comment Period Start Date:</b>	12/12/2016
<b>Comment Period End Date:</b>	1/25/2017
<b>Associated Ballots:</b>	2016-02 Modifications to CIP Standards CIP-003-7(i) Implementation Plan IN 1 OT 2016-02 Modifications to CIP Standards CIP-003-7(i) IN 1 ST 2016-02 Modifications to CIP Standards Removable Media   New Definition IN 1 DEF 2016-02 Modifications to CIP Standards Transient Cyber Asset   New Definition IN 1 DEF

There were 50 sets of responses, including comments from approximately 136 different people from approximately 110 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the [project page](#).

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Director of Standards Development, [Steve Noess](#) (via email) or at (404) 446-9691.

## Questions

- 1. Definition: The SDT revised the definition of Transient Cyber Asset 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.**
- 2. Definition: The SDT revised the definition of Removable Media 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-003-7(i), Attachment 1, adding Section 5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation to reflect the mandatory requirement for the Responsible Entity to develop and implement security plans to mitigate the risk of 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 evidential language of CIP-003-7(i), Attachment 2, Section 5 to make the Measures 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.**

## Questions

**6. Implementation Plan:** The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the standard, 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.**

**The Industry Segments are:**

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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Luminant - Luminant Energy	Brenda Hampton	6		Luminant	Brenda Hampton	Luminant - Luminant Energy	6	Texas RE
					Stewart Rake	Luminant Mining Company LLC	7	Texas RE
					Alshare Hughes	Luminant - Luminant Generation Company LLC	5	Texas RE
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
ACES Power Marketing	Brian Van Gheem	6	NA - Not Applicable	ACES Standards Collaborators	Bob Solomon	Hoosier Energy Rural Electric	1	RF

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Cooperative, Inc.		
					Shari Heino	Brazos Electric Power Cooperative, Inc.	1,5	Texas RE
					Ellen Watkins	Sunflower Electric Power Corporation	1	SPP RE
					Mark Ringhausen	Old Dominion Electric Cooperative	3,4	SERC
					Eric Jensen	Arizona Electric Power Cooperative, Inc.	1	WECC
					Ryan Strom	Buckeye Power, Inc.	4	RF
					Susan Sosbe	Wabash Valley Power Association	3	RF
Chris Gowder	Chris Gowder		FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					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
					Jeffrey Partington	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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	9	FRCC
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
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
	Ruida Shu	1,2,3,4,5,6,7,10	NPCC		Paul Malozewski	Hydro One.	1	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Northeast Power Coordinating Council				RSC no Dominion and OPG	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
					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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					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
					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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Chuck Lawrence	American Transmission Company	1	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
					Brad Parret	Minnesota Power	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service	3,5,6	MRO
					Jeremy Volls	Basin Electric Power Coop	1	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent Independent System Operator	2	MRO
Colorado Springs Utilities	Shannon Fair	6		Colorado Springs Utilities	Kaleb Brimhall	Colorado Springs Utilities	5	WECC
					Charlie Morgan	Colorado Springs Utilities	3	WECC
					Shawna Speer	Colorado Springs Utilities	1	WECC
					Shannon Fair	Colorado Springs Utilities	6	WECC
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Megan Wagner	Westar Energy	1,3,5,6	SPP RE

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Robert Gray	Board of Public Utilities (Kansas-BPU)	3	SPP RE
					Steve Keller	Southwest Power Pool Inc.	2	SPP RE
					Tony Eddleman	Nebraska Public Power District	1,3,5	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
					Paul Camilletti	Santee Cooper	5	SERC
					Bob Rhett	Santee Cooper	5	SERC
					Mike Frederick	Santee Cooper	1	SERC
					Troy Lee	Santee Cooper	1	SERC

**Summary of Changes**

Spelling, formatting, and other errors were corrected.

**CIP-003-7(i):**

Based on stakeholder comments, the SDT made non-substantive changes to the standard, primarily in the Guidelines and Technical Basis section to provide additional clarity.

**Implementation Plan:**

No changes made.

**Definitions of Transient Cyber Asset and Removable Media:**

No changes made.

**1. Definition: The SDT revised the definition of Transient Cyber Asset 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.**

**Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC**

**Answer** No

**Document Name**

**Comment**

Seattle City Light has concerns that the revised definition of Transient Cyber Asset is not consistent with the risk-based approach reflected in the NERC CIP version 5/6 Standards. In particular Seattle finds the revised definition is inconsistent with the language of CIP-002-5.1 R1.3 regarding identification of BES Cyber Systems (and by extension BES Cyber Assets) at Low impact facilities, specifically that: “a discrete list of low impact BES Cyber Systems is not required.” Given that the proposed definition defines Transient Cyber Assets in terms of BES Cyber Assets and BES Cyber Systems, Seattle does not understand how the existence of any low impact Transient Cyber Asset can be documented or audited absent a list of such BES Cyber Systems or Assets. Seattle is further concerned that the revised definition could lead to a requirement to produce such lists, which previously has been deemed not consistent with the risk-based approach adopted in CIP version 5/6 (because the development and accurate maintenance of such lists would consume large resources that would provide greater benefits to cyber security if applied elsewhere). At this time Seattle does not have alternative language to suggest to resolve this conundrum, which is inherent to the structure of CIP version 5/6. Perhaps a revision of the definition for Low impact Transient Cyber Asset to reference only a temporary connection “to a BES Cyber System at a low impact facility” might work, but Seattle remains unconvinced that such a definition would prove auditable.

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

Although the definition of Transient Cyber Asset (TCA) references BES Cyber Assets (BCA), a discrete list of BCAs or BES Cyber Systems is not required; However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact

BES Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any Transient Cyber Asset prior to connecting it to a low impact BES Cyber System(s). The security objective of the requirement is to mitigate the risk of introducing malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The requirement lists options but the Responsible Entity has the discretion as to how it satisfies the security objective.

#### Julie Hall - Entergy - 6

**Answer** No

**Document Name**

#### Comment

The proposed definition of Transient Cyber Asset (TCA) implies additional requirements for entities to comply with that is in misalignment with standards that are currently approved and in effect. The purpose of CIP-003-7(i) is to create TCA requirements for Low Impact BES Cyber Systems, yet none of the criteria of item 4 of the definition can be achieved for Lows without imposing additional, and improper, requirements upon the Registered Entities. Item 4 bullets 2 and 3 are omitted because they explicitly require the device or network to be associated with a high or medium impact, leaving just the direct connection to a BES Cyber Asset as the required #4 criteria. However, CIP-002-5.1 R1.3 reads “Identify each asset that contains a low impact BES Cyber System according...if any (a discrete list of low impact BES Cyber Systems is not required).” The requirement explicitly states that a discrete list of BES Cyber Systems is not required. BES Cyber Systems are defined as “One or more BES Cyber Assets logically grouped”, showing that BES Cyber Assets are a sub-component of a BES Cyber System. CIP-002-5.1 explicitly states that a list of low impact BCS is not required, yet this definition of TCA would require entities to evaluate and inventory, and maintain that inventory, to identify every BES Cyber Asset in order to correctly identify TCA that could be used at a low impact site. Entergy proposes some verbiage to include low impact BCS, while not adding additional inventorying requirements such as “Anticipated for use within a low impact BCS, if any”.

Likes 0

Dislikes 0

#### Response

Thank you for your comment.

Although the definition of Transient Cyber Asset (TCA) references BES Cyber Assets (BCA), a discreet list of BCAs or BES Cyber Systems is not required; However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any Transient Cyber

Asset prior to connecting it to a low impact BES Cyber System(s). The security objective of the requirement is to mitigate the risk of introducing malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The requirement lists options but the Responsible Entity has the discretion as to how it satisfies the security objective. The SDT declines to make the suggested change because it would broaden the scope of the definition and present difficulties in identifying TCAs based on anticipated intent.

**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**

Since PCA is already defined by NERC, NRG recommends deleting associated with high or medium impact BES Cyber Systems since “associated” could be misunderstood and appears to be redundant. For example, would a VPN connection be considered a TCA? (i.e. connecting at layer 3 or below)

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

The definitions of PCA and ESP in the published glossary of term does not infer high, medium or low impact categorization. The purpose of the word "associated" with high or medium impact BES Cyber Systems is meant to qualify the impact category of the BES Cyber System and its associated PCA and ESP used in the TCA definition. A VPN connection would not be considered a TCA as it would not be directly connected to a Cyber Asset as item 4 in the definition of TCA specifies.

<b>Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<ol style="list-style-type: none"> <li>1. We feel the SDT's approach to revise the definition of Transient Cyber Assets (TCA), such that it is relevant to the controls required for high, medium, and low impact BES Cyber Systems, is inconsistent with the directives listed within FERC Order No. 822. These directives focus on the high and medium impact BES Cyber Security requirements. However, the proposed revisions implicitly require low impact entities to have the same level of risk mitigations in places as if they were associated with high and medium impact BES Cyber Systems. We believe the SDT should avoid the inclusion of low impact BES Cyber Systems entirely or provide proof of a risk analysis to substantiate this activity.</li> <li>2. The SDT's proposed approach will also create difficulty for industry to demonstrate compliance since a BES Cyber System's inventory list is not required for low impact entities. How are auditors able to benchmark a low impact entity's compliance program without a current list?</li> <li>3. We suggest the SDT consider another method to address the FERC directive that still preserves the low impact requirements and the explicit exclusion from being required to have an inventory list of low impact assets. Such an approach could include TCAs in the technical guidance under Electronic Access Controls.</li> <li>4. Another possible approach is for low impact entities to have a documented process that applies electronic access controls for TCAs to low impact assets. <ol style="list-style-type: none"> <li>i. Auditors could verify that the entity has developed the documented process, and the entity could demonstrate compliance by providing the document as evidence.</li> <li>ii. This approach also preserves the disparate treatment of low and medium impact assets by assigning different requirement levels that commensurate with BES level risks.</li> </ol> </li> </ol>	
Likes	0
Dislikes	0

**Response**

Thank you for your comments.

1. In Order 822 paragraph 32, FERC directs that the CIP standards be modified to "provide mandatory protection for transient devices used at low impact BES Cyber Systems based on the risk posed to Bulk Electric System reliability." The SDT asserts that TCA's connected to low impact BES Cyber Systems must be included to meet the intent of this directive. The SDT asserts that the lower risk of lows was considered and the resulting requirements applied to TCA's that connect to low impact BES Cyber Systems are not as stringent as those for TCA's connected to medium and high impact BES Cyber Systems.

2. In paragraph 36 of Order 822, FERC supports that the controls can "avoid overly burdensome administrative tasks that could be associated with identifying discrete Low Impact BES Cyber Assets" and the standard continues to not require inventories of discrete low impact BES Cyber Assets. The SDT cannot comment on how auditors may approach checking an entity's compliance but in no event is a list of low impact BES Cyber Systems required.

3. Electronic access controls are required to protect external connectivity using routable protocols to the asset; e.g. substation (not connections within the asset or at the individual Cyber Asset level). The SDT disagrees that the electronic access controls section of an entity's plan should mix asset and Cyber Asset level connectivity.

4. The requirement is to have a documented plan as you suggest, but the plan would not address electronic access controls for TCAs. The relevant section of the plan for TCAs should address mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media.

**Ronald Donahey - TECO - Tampa Electric Co. - 3**

<b>Answer</b>	No
<b>Document Name</b>	

**Comment**

Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Transient Cyber Asset definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.

The definition does not spell out what defines a TCA in a low impact environment. Should the definition include additional instruction related to item 4 such as “connected to a cyber asset located in an asset containing low impact BES Cyber Systems”?

Likes 0

Dislikes 0

**Response**

Thank you for your comments.

1. In Order 822 paragraph 32, FERC directs that the CIP standards be modified to "provide mandatory protection for transient devices used at low impact BES Cyber Systems based on the risk posed to Bulk Electric System reliability." The SDT asserts that TCA's connected to low impact BES Cyber Systems must be included to meet the intent of this directive. The SDT asserts that the lower risk of lows was considered and the resulting requirements applied to TCA's that connect to low impact BES Cyber Systems are not as stringent as those for TCA's connected to medium and high impact BES Cyber Systems.

2. In paragraph 36 of Order 822, FERC supports that the controls can "avoid overly burdensome administrative tasks that could be associated with identifying discrete Low Impact BES Cyber Assets" and the standard continues to not require inventories of discrete low impact BES Cyber Assets. The SDT cannot comment on how auditors may approach checking an entity's compliance but in no event is a list of low impact BES Cyber Systems required.

3. Electronic access controls are required to protect external connectivity using routable protocols to the asset; e.g. substation (not connections within the asset or at the individual Cyber Asset level). The SDT disagrees that the electronic access controls section of an entity's plan should mix asset and Cyber Asset level connectivity.

4. The requirement is to have a documented plan as you suggest, but the plan would not address electronic access controls for TCAs. The relevant section of the plan for TCAs should address mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media.

**Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov**

**Answer**

No

**Document Name**

**Comment**

In the current TCA definition, section 4, first bullet: If the intent of the definition for “BES Cyber Asset” to be applicable for all three impact classifications (High, Medium, and Low), then SDG&E recommends adding this clarification.

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

The SDT contends the definition needs to describe what a TCA is regardless of its impact rating. Impact ratings are taken into account within respective requirements for highs, mediums, and lows.

**Shannon Fair - Colorado Springs Utilities - 6, Group Name** Colorado Springs Utilities

**Answer**

Yes

**Document Name**

**Comment**

Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Transient Cyber Asset definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

The SDT included the referenced language in the definitions to specifically address the fact that ESPs and PCAs are not required to be identified at assets containing low impact BES Cyber Systems. No additional guidance is required.

<b>Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Duke Energy would like to point out a possible typo on page 3 of the Proposed Definitions of: Transient Cyber Asset”(TCA) and “Removable Media” document. The title of the section on page 3 reads “Currently Approved Definition of Transient Cyber Asset (TCS)”. The definition below is actually the definition of Removable Media. The title appears to be incorrect. We recommend the drafting team change the title to read: “ <i>Currently Approved Definition of Removable Media</i> ”.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment.	
The SDT made the modification.	
<b>Bob Thomas - Illinois Municipal Electric Agency - 4</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.	
Likes	0
Dislikes	0

Response	
Please see the SDT's responses to comments submitted by APPA.	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes	0
Dislikes	0
Response	
Please see the SDT's responses to comments submitted by APPA.	
Roger Dufresne - Hydro-Quebec Production - 5	
Answer	Yes
Document Name	
Comment	
<p>Add a « Low impact BES » item in the TCA definition. This will exempt the inventory requirement for low to demonstrate compliance for the TCA.</p> <p>The proposed definition of a Transient Cyber Asset (TCA) is:</p> <p><i>A Cyber Asset that is:</i></p> <ol style="list-style-type: none"> <li><i>1. capable of transmitting or transferring executable code,</i></li> <li><i>2. not included in a BES Cyber System,</i></li> <li><i>3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and</i></li> </ol>	

4. *directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:*

*BES Cyber Asset,*

*Add "Low impact BES Cyber System",*

*network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*

*PCA associated with high or medium impact BES Cyber Systems.*

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

The definition of Transient Cyber Asset (TCA) references BES Cyber Assets (BCAs) regardless of impact level. A BES Cyber System is defined as "One or more BES Cyber Assets..." therefore, the SDT disagrees with adding the proposed text.

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

Answer

Yes

Document Name

**Comment**

It would be helpful if the revised definitions could be reorganized to provide the inclusions first and the exclusions second to make them easier to read and implement. For example, the TCA definition could be changed to:

"A Cyber Asset that is: 1) capable of transmitting or transferring executable code; 2) directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: BES Cyber Asset, network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or PCA associated with high or medium impact BES Cyber Systems; 3) not included in a BES Cyber System; and 4) not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems. Examples..."

Also, the applicability of the definitions to LIBCS is not clear, we recommend changing “BES Cyber Asset” in bullet 4 for each definition to “BES Cyber System” or alternatively “low, medium, or high impact BES Cyber System.”

Likes 0

Dislikes 0

**Response**

Thank you for your comments.

The revisions to the definitions were only to clarify applicability to low impact. The structure is consistent with the currently approved definition. The definition of Transient Cyber Asset (TCA) references BES Cyber Assets (BCAs) regardless of impact level. A BES Cyber System is defined as "One or more BES Cyber Assets..." therefore, the SDT disagrees that adding the proposed text or rearranging the order of the definition would improve clarity.

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

**Answer**

Yes

**Document Name**

**Comment**

Suggest to add a « Low impact BES » item in the TCA definition. This will exempt the inventory requirement for low to demonstrate compliance for the TCA.

The proposed definition of a Transient Cyber Asset (TCA) is:

*A Cyber Asset that is:*

1. *capable of transmitting or transferring executable code,*
2. *not included in a BES Cyber System,*
3. *not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and*

4. *directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:*

- *BES Cyber Asset,*
- *Add “Low impact BES Cyber System”,*
- *network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*
- *PCA associated with high or medium impact BES Cyber Systems.*

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

The definition of Transient Cyber Asset (TCA) references BES Cyber Assets (BCAs) regardless of impact level. A BES Cyber System is defined as "One or more BES Cyber Assets..." therefore, the SDT disagrees with adding the proposed text.

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

Answer Yes

Document Name

**Comment**

Santee Cooper agrees with APPA's comment/concern.

Likes 0

Dislikes 0

**Response**

Please see the SDT’s responses to comments submitted by APPA.

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, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; 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 FMMPA

Answer Yes

Document Name

Comment

Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Transient Cyber Asset definition. Guidance would show that low impact BES Cyber Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.

Likes 0

Dislikes 0

Response

Thank you for your comment.

The SDT included the referenced language in the definitions to specifically address the fact that ESPs and PCAs are not required to be identified at assets containing low impact BES Cyber Systems. No additional guidance is required.

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

<b>Response</b>	
<b>RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Christopher Chavez - Salt River Project - 1,3,5,6 - WECC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	

<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Bobby Olsen - Salt River Project - 6</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1,3</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Michael Ward - Seminole Electric Cooperative, Inc. - 4</b>	
<b>Answer</b>	Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Karie Barczak - DTE Energy - Detroit Edison Company - 3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	

<b>Response</b>	
<b>Sean Bodkin - Dominion - Dominion Resources, Inc. - 6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Ryan Olson - Portland General Electric Co. - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Chris Scanlon - Exelon - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	

<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Jason Snodgrass - Georgia Transmission Corporation - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Stephanie Little - APS - Arizona Public Service Co. - 5</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>David Gordon - Massachusetts Municipal Wholesale Electric Company - 5</b>	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Mike Anctil - Los Angeles Department of Water and Power - 3</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Wendy Center - U.S. Bureau of Reclamation - 5</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Rachel Coyne - Texas Reliability Entity, Inc. - 10</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Patricia Lynch - NRG - NRG Energy, Inc. - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Likes	0
Dislikes	0
<b>Response</b>	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion and OPG	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Glen Farmer - Avista - Avista Corporation - 1,3,5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	

Dislikes 0

**Response**

**2. Definition: The SDT revised the definition of Removable Media 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.**

**Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov**

**Answer** No

**Document Name**

**Comment**

In the proposed Removable Media definition, section 4, first bullet: If the intent of the definition for “BES Cyber Asset” to be applicable for all three impact classifications (High, Medium, and Low), then SDG&E recommends adding this clarification.

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

The SDT contends the definition needs to describe what Removable Media is regardless of its impact rating. Impact ratings are taken into account within respective requirements for highs, mediums, and lows.

**Ronald Donahey - TECO - Tampa Electric Co. - 3**

**Answer** No

**Document Name**

**Comment**

Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP’s and PCA’s to the Removable Media definition. Guidance would show that low impact BES Cyber Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified. The definition does not spell out what defines RM in a low impact environment. Should the definition include additional instruction related to item 4 such as “connected to a cyber asset located in an asset containing low impact BES Cyber Systems”?

Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment.	
The SDT included the referenced language in the definitions to specifically address the fact that ESPs and PCAs are not required to be identified at assets containing low impact BES Cyber Systems. No additional guidance is required.	
<b>Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name</b> ACES Standards Collaborators	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<ol style="list-style-type: none"> <li>1. Similar to TCAs, we suggest the SDT revise its approach and remove low impact BES Cyber Security requirements from the definition of Removable Media (RM). We feel its relevance on controls required for high, medium, and low impact BES Cyber Systems is not the best way to address the directives listed in FERC Order No. 822. The proposed revisions implicitly require low impact entities to have the same level of risk mitigations in places as if they were associated with high and medium impact BES Cyber Systems. We believe the SDT should avoid the inclusion of low impact BES Cyber Systems entirely or provide proof of a risk analysis to substantiate this activity.</li> <li>2. We suggest the SDT consider another method to address the FERC directive that still preserves the low impact requirements and the explicit exclusion from being required to have an inventory list of low impact assets. Such an approach could include Removable Media in the technical guidance under Electronic Access Controls that are currently approved.</li> <li>3. One possible approach is for low impact entities to have a documented process that applies electronic access controls for Removable Media to low impact assets.             <ol style="list-style-type: none"> <li>i. Auditors could verify that the entity has developed the documented process, and the entity could demonstrate compliance by providing the document as evidence.</li> <li>ii. This approach also preserves the disparate treatment of low and medium impact assets by assigning different requirement levels that commensurate with BES level risks</li> </ol> </li> </ol>	

Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comments.	
<p>1. In Order 822 paragraph 32, FERC directs that the CIP standards be modified to ""provide mandatory protection for transient devices used at low impact BES Cyber Systems based on the risk posed to Bulk Electric System reliability."" The SDT asserts that Removable Media connected to low impact BES Cyber Systems must be included as a transient device to meet the intent of this directive.</p> <p>2. In paragraph 36 of Order 822, FERC supports that the controls can "avoid overly burdensome administrative tasks that could be associated with identifying discrete Low Impact BES Cyber Assets" and the standard continues to not require inventories of discrete low impact BES Cyber Assets. The SDT cannot comment on how auditors may approach checking an entity's compliance, but a list of low impact BES Cyber Systems is not required.</p> <p>3. The requirement is to have a documented plan as you suggest, but the plan would not address electronic access controls for Removable Media. The relevant section of the plan for Removable Media should address mitigating the risk of the introduction of malicious code into low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media.</p>	
<b>Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Since PCA is already defined by NERC, NRG recommends deleting associated with high or medium impact BES Cyber Systems since "associated" could be misunderstood and appears to be redundant.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment.	

The definitions of PCA and ESP in the published glossary of term does not infer high, medium or low impact categorization. The purpose of the word "associated" with high or medium impact BES Cyber Systems is meant to qualify the impact category of the BES Cyber System and its associated PCA and ESP used in the Removable Media definition. The SDT included the referenced language specifically to address the fact that ESPs and PCAs are not required to be identified at assets containing low impact BES Cyber Systems.

**Julie Hall - Entergy - 6**

**Answer**

No

**Document Name**

**Comment**

The proposed definition of Removable Media (RM) implies additional requirements for entities to comply with that is in misalignment with standards that are currently approved and in effect. The purpose of CIP-003-7(i) is to create RM requirements for Low Impact BES Cyber Systems, yet none of the criteria of item 4 of the definition can be achieved for Lows without imposing additional, and improper, requirements upon the Registered Entities. Item 4 bullets 2 and 3 are omitted because they explicitly require the device or network to be associated with a high or medium impact, leaving just the direct connection to a BES Cyber Asset as the required #4 criteria. However, CIP-002-5.1 R1.3 reads “Identify each asset that contains a low impact BES Cyber System according...if any (a discrete list of low impact BES Cyber Systems is not required).” The requirement explicitly states that a discrete list of BES Cyber Systems is not required. BES Cyber Systems are defined as “One or more BES Cyber Assets logically grouped”, showing that BES Cyber Assets are a sub-component of a BES Cyber System. CIP-002-5.1 explicitly states that a list of low impact BCS is not required, yet this definition of TCA would require entities to evaluate and inventory, and maintain that inventory, to identify every BES Cyber Asset in order to correctly identify RM that could be used at a low impact site. Entergy proposes some verbiage to include low impact BCS, while not adding additional inventorying requirements such as “Anticipated for use within a low impact BCS, if any”.

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

Although the definition of Removable Media references BES Cyber Assets (BCA), a discrete list of BCAs or BES Cyber Systems is not required; However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any Removable Media prior

to connecting it to a low impact BES Cyber System(s). The security objective of the requirement is to mitigate the risk of introducing malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The requirement lists options but the Responsible Entity has the discretion as to how it satisfies the security objective. The SDT declines to make the suggested change because it would broaden the scope of the definition and present difficulties in identifying Removable Media based on anticipated intent.

**Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC**

<b>Answer</b>	No
---------------	----

<b>Document Name</b>	
----------------------	--

**Comment**

As is the case for the revised Transient Cyber Asset definition, Seattle City Light has concerns that the revised definition of Removable Media is not consistent with the risk-based approach reflected in the NERC CIP version 5/6 Standards. In particular Seattle finds the revised definition is inconsistent with the language of CIP-002-5.1 R1.3 regarding identification of BES Cyber Systems (and by extension BES Cyber Assets) at Low impact facilities, specifically that: “a discrete list of low impact BES Cyber Systems is not required.” Given that the proposed definition defines Removable Media in terms of BES Cyber Assets and BES Cyber Systems, Seattle does not understand how the existence of any low impact Removable Media can be documented or audited absent a list of such BES Cyber Systems or Assets. Seattle is further concerned that the revised definition could lead to a requirement to produce such lists, which previously has been deemed not consistent with the risk-based approach adopted in CIP version 5/6 (because the development and accurate maintenance of such lists would consume large resources that would provide greater benefits to cyber security if applied elsewhere). At this time Seattle does not have alternative language to suggest to resolve this conundrum, which is inherent to the structure of CIP version 5/6. Perhaps a revision of the definition for Low impact Removable Media to reference only a temporary connection “to a BES Cyber System at a low impact facility” might work, but Seattle remains unconvinced that such a definition would prove auditable.

Likes 0	
---------	--

Dislikes 0	
------------	--

**Response**

Thank you for your comment.

Although the definition of Removable Media references BES Cyber Assets (BCA), a discreet list of BCAs or BES Cyber Systems is not required; However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES

Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any Removable Media prior to connecting it to a low impact BES Cyber System(s). The security objective of the requirement is to mitigate the risk of introducing malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The requirement lists options but the Responsible Entity has the discretion as to how it satisfies the security objective.

**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, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; 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 FMPPA**

Answer	Yes
Document Name	
<b>Comment</b>	
Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Removable Media definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment.	
The SDT included the referenced language in the definitions to specifically address the fact that ESPs and PCAs are not required to be identified at assets containing low impact BES Cyber Systems. No additional guidance is required.	
<b>Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper</b>	
Answer	Yes
Document Name	

**Comment**

Santee Cooper agrees with APPA's comment/concern.

Likes 0

Dislikes 0

**Response**

Please see the SDT's responses to comments submitted by APPA.

**Si Truc Phan - Hydro-Quebec TransEnergie - 1 - NPCC**

Answer

Yes

Document Name

**Comment**

Suggest to add a « Low impact BES » item in the TCA definition. This will exempt the inventory requirement for low to demonstrate compliance for the TCA.

The proposed definition of Removable Media is:

*Storage media that:*

1. *are not Cyber Assets,*
2. *are capable of transferring executable code,*
3. *can be used to store, copy, move, or access data, and*
4. *are directly connected for 30 consecutive calendar days or less to a:*
  - o *BES Cyber Asset,*
  - o *Low impact BES Cyber System,*
  - o *network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*

- o *Protected Cyber Asset associated with high or medium impact BES Cyber Systems.*

Likes 0

Dislikes 0

### Response

Thank you for your comment.

The definition of Removable Media references BES Cyber Assets (BCAs) regardless of impact level. A BES Cyber System is defined as "One or more BES Cyber Assets..." therefore, the SDT disagrees with adding the proposed text.

### Roger Dufresne - Hydro-Quebec Production - 5

Answer

Yes

Document Name

### Comment

Add a « Low impact BES » item in the TCA definition. This will exempt the inventory requirement for low to demonstrate compliance for the TCA.

The proposed definition of Removable Media is:

*Storage media that:*

- 5. are not Cyber Assets,*
- 6. are capable of transferring executable code,*
- 7. can be used to store, copy, move, or access data, and*
- 8. are directly connected for 30 consecutive calendar days or less to a:*  
*BES Cyber Asset,*  
*Low impact BES Cyber System,*

*network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or Protected Cyber Asset associated with high or medium impact BES Cyber Systems.*

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

The definition of Removable Media references BES Cyber Assets (BCAs) regardless of impact level. A BES Cyber System is defined as "One or more BES Cyber Assets..." therefore, the SDT disagrees with adding the proposed text.

**John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1**

**Answer**

Yes

**Document Name**

**Comment**

Tacoma Power supports comments submitted by APPA.

Likes 0

Dislikes 0

**Response**

Please see the SDT's responses to comments submitted by APPA.

**Bob Thomas - Illinois Municipal Electric Agency - 4**

**Answer**

Yes

**Document Name**

**Comment**

Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.

Likes 0

Dislikes	0
<b>Response</b>	
Please see the SDT's responses to comments submitted by APPA.	
<b>Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Removable Media definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment.	
The SDT included the referenced language specifically to address the fact that ESPs and PCAs are not required to be identified at assets containing low impact BES Cyber Systems.	
<b>Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino</b>	
Answer	Yes
Document Name	

**Comment**

The term “transferring code” is misleading because the device itself (for example, storage media) cannot transfer code without assistance from the host computer.

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

As stated in the definition, the Removable Media is capable of transferring executable code regardless of whether the host computer assists or not; consequently, no changes to the definition are necessary.

**Glen Farmer - Avista - Avista Corporation - 1,3,5**

**Answer**

Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

**Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6**

**Answer**

Yes

**Document Name**

**Comment**

Likes	0
Dislikes	0
<b>Response</b>	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion and OPG	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Patricia Lynch - NRG - NRG Energy, Inc. - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	

Dislikes 0	
<b>Response</b>	
<b>Wendy Center - U.S. Bureau of Reclamation - 5</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Mike Anctil - Los Angeles Department of Water and Power - 3</b>	
Answer	Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>David Gordon - Massachusetts Municipal Wholesale Electric Company - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Karie Barczak - DTE Energy - Detroit Edison Company - 3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	

<b>Response</b>	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF	
Answer	Yes
Document Name	

<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	

<b>Response</b>	
<b>Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Jason Snodgrass - Georgia Transmission Corporation - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	

<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Chris Scanlon - Exelon - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Ryan Olson - Portland General Electric Co. - 5</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Sean Bodkin - Dominion - Dominion Resources, Inc. - 6</b>	
Answer	Yes
Document Name	
<b>Comment</b>	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Michael Ward - Seminole Electric Cooperative, Inc. - 4</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1,3</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Bobby Olsen - Salt River Project - 6</b>	
Answer	Yes
Document Name	
Comment	

Likes	0
Dislikes	0
<b>Response</b>	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jamie Monette - Allete - Minnesota Power, Inc. - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Rachel Coyne - Texas Reliability Entity, Inc. - 10</b>	
<b>Answer</b>	
<b>Document Name</b>	

**Comment**

Texas RE noticed the TCA definition includes examples of what directly connected means, *“directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a”*.

There are no examples for “directly connected” listed in the Removable Media definition. Texas RE recommends that the SDT provide examples to provide clarity to the industry. There are instances when removable media may be physically directly connected but not active until mounted.

Likes	0
Dislikes	0

**Response**

Thank you for your comment.

The SDT contends that examples of “directly connected” are not necessary for Removable Media. The entity should scan all Removable Media prior to connecting to the BCA whether the Removable Media is mounted or not.

**3. Requirement R2: The SDT revised CIP-003-7(i), Attachment 1, adding Section 5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation to reflect the mandatory requirement for the Responsible Entity to develop and implement security plans to mitigate the risk of 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.**

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

Answer No

Document Name

Comment

The NSRF clearly understands that all entities regardless of size can be the door way for malicious code to entire into the BES systems. This includes small entities with one Low Impact BES Cyber Systems only (read low risk) (maybe a generator, one Transmission sub station, or control system). With this is mind, the NSRF has the following concerns that the SDT should clarify for all entities with Low Impact BES Cyber Systems.

The NSRF has concerns with Attachment 1, part 5.2 for entities that have Low Impact BES Cyber Systems, only. The actionable items in 5.2 is for us the entity to “Review” items that the “other party” needs to do to do prior to connecting to our Low Impact BES Cyber System. Please clariy what “review” means? What is acceptable within our review process? Attachment 2 states examples of electronic mail, policies, contracts, etc. Do we just review that the “other party” states that they will accomplish the attributes of 5.2 and have that stated within a contract, e-mail, STOW, etc. and we are compliant? This will play a role with proprietary software when a vendor will not provide associated evidence.

This clarity will reduce the compliance risks for the small entity and will assure that entities meet the attributes of 5.2, thus maintaining a secure BPS.

**5.1 For Transient Cyber Asset(s)** managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

&bull; Antivirus software, including manual or managed updates of signatures or patterns;

&bull; Application whitelisting; or

• Other method(s) to mitigate the introduction of malicious code.

Please clarify how the SDT wishes to use the semicolon within the first bullet of 5.1? Does this mean “and” or “or” as in the second bullet? We have the same question for all semicolons in 5.2 as well. The NSRF believes by adding a simple “or” after each semicolon, we will clearly know what the intent of the bulleted items are.

Likes 1	Georgia Transmission Corporation, 1, Snodgrass Jason
---------	--

Dislikes 0	
------------	--

**Response**

Thank you for your comments.

Specific approaches on how to perform the review could be submitted as Implementation Guidance in accordance with NERC Compliance Guidance Policy.

According to the background sections of the CIP standards, the use of the semicolon and the "or" is consistent with the usage in all standards. A bulleted list means an "or" and a numbered list means "and."

**Michael Ward - Seminole Electric Cooperative, Inc. - 4**

Answer	No
--------	----

Document Name	
---------------	--

**Comment**

The language is open ended and fails to provide discrete direction to entities on how to implement a plan. This will lead to subjective enforcement, with the possibility for significant discrepancies and differences between regions.

Likes 0	
---------	--

Dislikes 0	
------------	--

Response	
Thank you for your comment.	
The SDT notes that the requirement allows entities the flexibility to develop and implement the plan(s) appropriate for the entity's environment.	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
Seattle City Light agrees with the revisions so far as they go, but finds that they do not address the question of what would be acceptable evidence of the existence of any Low impact Transient Cyber Asset (based on the proposed definition) in the absence of an explicit list of Low impact BES Cyber Systems and Assets at a facility. As discussed in the definition comment above, Seattle does not have a solution to the problem, which is inherent to the structure of CIP verion 5/6.	
Likes 0	
Dislikes 0	
Response	
Please see the SDT's responses to your Question 1 comment.	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
This is a low impact requirement rather than a high or medium impact requirement. While risks of malicious code are definitely present, the reduced risk level would make this entire requirement more effective by requiring the entity document and implement a security program with appropriate controls that prevent introduction of malicious code. Examples of appropriate controls are: application	

whitelisting, antivirus, use of bootable CDs without known malware, contracts with vendors, etc. Note that use of third party TCA is expected to be much more frequent on low impact BCS and highly prescriptive requirements are less effective.

Should the above approach not be acceptable, requirement 5.3.1 and 5.3.2 should be consolidated into a single statement. A requirement to scan prior to connecting and then separately document and mitigate is redundant. The Removable media simply needs to be clean prior to connecting to a Transient Cyber Asset. Seminole suggests making that the requirement.

For example, the language could be modified to state:

For Removable Media, document and implement methods that prevent the introduction of malicious code on BES Cyber Assets when connecting Removable Media. In cases of detected malicious code that cannot be removed, the entity shall document how the identified malware is mitigated.

Likes	0
-------	---

Dislikes	0
----------	---

**Response**

Thank you for your comment.

The SDT notes that the requirement allows entities to implement a security program as suggested by your comment and includes the flexibility to develop a single plan for implementing Attachment 1, Sections 5.3.1 and 5.3.2.

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

Answer	No
--------	----

Document Name	
---------------	--

**Comment**

ITC Holdings agrees with the comment submitted by NSRF – see below:

The NSRF clearly understands that all entities regardless of size can be the door way for malicious code to entire into the BES systems. This includes small entities with one Low Impact BES Cyber Systems only (read low risk) (maybe a generator, one Transmission sub station, or control system). With this is mind, the NSRF has the following concerns that the SDT should clarify for all entities with Low

### Impact BES Cyber Systems.

The NSRF has concerns with Attachment 1, part 5.2 for entities that have Low Impact BES Cyber Systems, only. The actionable items in 5.2 is for us the entity to “Review” items that the “other party” needs to do prior to connecting to our Low Impact BES Cyber System. Please clarify what “review” means? What is acceptable within our review process? Attachment 2 states examples of electronic mail, policies, contracts, etc. Do we just review that the “other party” states that they will accomplish the attributes of 5.2 and have that stated within a contract, e-mail, STOW, etc. and we are compliant? This will play a role with proprietary software when a vendor will not provide associated evidence.

This clarity will reduce the compliance risks (burden) for the small entity and will assure that entities meet the attributes of 5.2.

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

Please clarify how the SDT wishes to use the semicolon within the first bullet of 5.1? Does this mean “and” or “or” as in the second bullet? We have the same question for all semicolons in 5.2 as well. The NSRF believes by adding a simple “or” after each semicolon, we will clearly know what the intent of the bulleted items are.

Likes	0	
Dislikes	0	

Response	
<p>Thank you for your comments.</p> <p>Specific approaches on how to perform the review could be submitted as Implementation Guidance in accordance with NERC Compliance Guidance Policy.</p> <p>According to the background sections of the CIP standards, the use of the semicolon and the "or" is consistent with the usage in all standards. A bulleted list means an "or" and a numbered list means "and."</p>	
<p><b>David Gordon - Massachusetts Municipal Wholesale Electric Company - 5</b></p>	
Answer	No
Document Name	
<p><b>Comment</b></p> <p>MMWEC supports the comments submitted by Georgia Transmission Corp. regarding streamling Section 5 by moving the bullets to GTB and keeping the security objective in the Attachment.</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comments.</p> <p>The use of the bulleted list is consistent with other currently approved standards. The SDT's intention in using the bulleted list is to provide options to satisfy the parent statement, and the SDT purposely included the ability for the Responsible Entity to use other protection methods, rather than those listed, that more adequately fit the entity's environment.</p>	
<p><b>Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators</b></p>	
Answer	No
Document Name	
<p><b>Comment</b></p>	

1. We have concerns with part 5.2 of Attachment 1 for applicable entities that only have Low Impact BES Cyber Systems. Many of these entities provide a small risk to the BES since they only have one low impact BES Cyber Systems (e.g. a generator, one Transmission substation, or a single control system). Will Regional Entities conduct the same audit for small entities as they would for large multi-regional corporate companies? What is the impact when a vendor does not comply with the request listed in part 5.2?
2. We also question the need for additional explicit requirements to validate vendor security and patch management plans as part of a low impact entity's cyber security policies. We believe these requirements are already incorporated in an entity's Electronic Access Controls Policy. These additional requirements are a burden to existing low impact entities that may only have one or two TCA-applicable or RM-applicable BES cyber assets. We recommend removing these requirements for low Impact entities until after the effective date for NERC Reliability Standard CIP-007-3 (i.e. September 1, 2018).
3. The inclusion of TCA and RM with the final definition of LERC is unnecessary. We don't agree with the SDT's approach of posting two options, and then recommend the all-inclusive option over the other. The SDT should wait for industry to provide feedback on both options or post only one path forward and determine if industry supports it. The one option adds additional risk for ballot approval.

Likes	0
Dislikes	0

### Response

Thank you for your comments.

The SDT cannot comment on the manner in which audits will be conducted by the Regional Entities. Compliance with the requirements is the responsibility of the entity being audited. In Attachment 1, Section 5, Part 5.2, the intention of the SDT is to provide options that a Responsible Entity can employ to ensure TCAs managed by third parties do not present additional risk to the BES. Please refer to example evidence in Attachment 2 for possible options.

If a Responsible Entity's Electronic Access Control Policy is able to mitigate the risk of the introduction of malware via TCAs, the Responsible Entity can utilize this as such and present that to auditors. The SDT intentionally ensured this requirement was not prescriptive to allow an entity to provide appropriate protections per their environment.

The SDT's objective is to minimize the number of revisions.	
<b>Mike Anctil - Los Angeles Department of Water and Power - 3</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
This NERC project is adding a new Section 5 bringing into scope Transient Cyber Assets and Removable Media for Low Impact Facilities which is a much larger scope than our High and Medium Impact Program without any extension of time for compliance indicated for implementation. This will be impactful to the Power System.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment.	
The intention of the SDT is to give Responsible Entities more flexibility at Lows than is currently allowed at Highs or Mediums while satisfying the FERC 822 directive. An entity can choose to utilize the same programs currently implemented for Highs and Mediums to meet the security objective for Lows. The implementation period for CIP-003-7(i) is 18 months.	
<b>Wendy Center - U.S. Bureau of Reclamation - 5</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Reclamation appreciates the Standards Drafting Team's consideration of prior recommendations. Reclamation agrees with the changes and has the following question:	
In this version of CIP-003-7(i), did the SDT intend to add guidance regarding the new section on page 9 under Requirement 1 "1.2.6 Declaring and responding to CIP Exceptional Circumstances" in Attachment 1 and/or Attachment 2?	
Likes	0

Dislikes 0

**Response**

Thank you for your comment.

The SDT added G&TB language for Requirement R1, Part 1.2.6.

**Rachel Coyne - Texas Reliability Entity, Inc. - 10****Answer**

No

**Document Name****Comment**

Texas RE's appreciates the SDT's efforts to implement the FERC directive in Order No. 822 to "develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to the bulk electric system reliability." In implementing this directive, Texas RE notes that the SDT appears to have used the existing Transient Cyber Asset (TCA) and Removable Media requirements for medium and high impact BES Cyber Systems and associated Protected Cyber Assets set forth in CIP-10-2, Attachment 1, Sections 1 through 3 as the basis for developing the new TCA and removable media requirements for low impact BES Cyber Systems.

While Texas RE agrees with this general approach, Texas RE notes that the SDT elected to not include all applicable requirements. For instance, the current draft of CIP-003, Attachment 1, Section 5 omits any requirements to mitigate software vulnerabilities (CIP-10-2, Attachment 1, Section 1.3 for TCAs managed by the Responsible Entity; CIP-10-2, Attachment 1, Section 2.1 for TCAs managed by a party other than the Responsible Entity). Texas RE requests that the SDT provide its risk-based justification for why those aspects of the CIP-010-2, Attachment 1 requirements for medium and high impact TCAs and removable media are not correspondingly extended to similar low impact devices. Among other things, this will assist Texas RE in its efforts to understand, evaluate, and ensure compliance with the new low impact requirements.

In addition, Texas RE noticed the following:

- There is no distinction provided for Removable Media used by different parties. Was that the intent of the SDT? As written it appears to be for any Removable Media used by any party (e.g., vendor, or third party technician/personnel).

- Texas RE recommends that the SDT specifically address the impact of backup tapes, libraries, and drives. More specifically Texas RE recommends addressing magnetic tapes, in regard to section 5.3.2. How would an entity mitigate the threat of detected malicious code on magnetic tapes prior to connecting it to a high, medium, or low impact BES Cyber System?
- On Page 29, Section 5 - Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation; there is an extra “\_” that is not needed after the colon symbol.

Likes 0

Dislikes 0

**Response**

Thank you for your comments.

In the assessment of risk, one factor is the impact or consequence of the realization of the risk. The SDT notes that the risk related to the introduction of malicious code is less for low impact BES Cyber Systems than medium or high impact BES Cyber Systems. This is because, by definition, the impact is less. As such, the SDT selected a reduced set of controls for low impact that directly address the concern that transient devices are potentially more susceptible to malicious code due to connections to different systems and networks. FERC Order 822 directed that the requirements be designed to effectively address the risks posed by transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards.

Yes, the intent of the SDT was not to create a distinction for third-party Removable Media. However, there is no language in Attachment 1 that would prevent an entity from making such a distinction in its own plan so long as the methods chosen meet the security objective identified in Section 5 of Attachment 1.

**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, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; 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 FMPPA**

Answer

No

Document Name

**Comment**

1) The bulleted list creates requirements that are too prescriptive. Use alternative language for Section 5.1 and 5.2 to remove the bullet points (because they may be used against you in some fashion in the future), and re-write the requirements. The bullet points should go into the GTB section so that there is less chance for a misinterpretation of reinterpretation that would require the implementation of more than one of the bulleted point in order to meet compliance.

2) As written, the requirements listed for TCAs in CIP-003-7(i) for Low Impact assets is a subset of the requirements for high and medium impact included in CIP-010-2 R4. As is or if changed the GTB section should include a statement the low impact requirements are a subset of those for High and Medium.

Likes 0

Dislikes 0

**Response**

Thank you for your comments.

The use of the bulleted list is consistent with other currently approved standards. The SDT's intention in using the bulleted list is to provide options to satisfy the parent statement, and the SDT purposely included the ability for the Responsible Entity to use other protection methods, rather than those listed, that more adequately fit the entity's environment.

The relationship between highs, mediums, and lows is addressed in Attachment 1 to allow entities to utilize a single program for all impact levels.

**Julie Hall - Entergy - 6**

**Answer**

Yes

**Document Name**

**Comment**

Agree with CIP-003-7(i), Attachment 1, Section 5 as written in this draft. As written, this verbiage implies entities has latitude to implement a strategy based on a risk to achieve the goal of the standard. See response to question 4 below for concerns regarding actual implementation of plans.

Likes 1	Georgia Transmission Corporation, 1, Snodgrass Jason
Dislikes 0	
<b>Response</b>	
Thank you for your comment.	
<b>Chris Scanlon - Exelon - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
<p>Exelon supports the changes made to CIP-003-7(i), R2, Attachment 1, adding Section 5; however, we request the SDT consider the following adjustments:</p> <ol style="list-style-type: none"> <li>The language in Attachment 1, Section 5, regarding “achieve the objective of mitigating the risk of the introduction of malicious code,” differs from the language in CIP-010-2, R4, Attachment 1, Section 1.3, which states “...achieves the objective of mitigating the introduction of...” Exelon requests the SDT consider aligning the two obligations to the language found in CIP-010-2, R4 or add clarification to the Guidelines and Technical Basis that provides clarity regarding the addition of “...the risk of...” and whether there are any additional or different expectations for Responsible Entities related to CIP-003-7(i), R2. Exelon is concerned that the addition of “risk” could be interpreted to require performing and documenting a risk assessment of all of the risks posed by the introduction of malicious code.</li> </ol> <p>The following sentence (or something comparative) could be added to the Guidelines and Technical Basis as the last sentence in the first paragraph related to Section 5.1 if the SDT determines the requirement language does not require alignment: “When determining the method(s) to mitigate the introduction of malicious code, it is not intended Responsible Entities have to perform and document a risk assessment to determine all of the risks associated with the introduction of malicious code.”</p> <ol style="list-style-type: none"> <li>Attachment 1, Section 5.3.2 states, “Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.” Exelon proposes a one-word change to replace the “...threat of...” to “...threat from...” This minor wording change helps to clarify the meaning of the obligation. Using the word “from” makes it clear that the mitigation of the threat is associated with already detected malicious code, as opposed to mitigation of a general threat of malicious code that may occur in the future.</li> </ol>	

Likes	0	
Dislikes	1	Georgia Transmission Corporation, 1, Snodgrass Jason
<b>Response</b>		
Thank you for your comments.		
The SDT does not intend for entities to perform a risk assessment and added the recommended language to the G&TB.		
The SDT asserts that the use of the word "and" at the end of Attachment 1, Section 5, Part 5.3.1 clarifies what is to be mitigated in Attachment 1, Section 5, Part 5.3.2.		
<b>Shannon Fair - Colorado Springs Utilities - 6, Group Name</b> Colorado Springs Utilities		
<b>Answer</b>	Yes	
<b>Document Name</b>		
<b>Comment</b>		
<p>1) The bulleted list creates requirements that are too prescriptive. Use alternative language for Section 5.1 and 5.2 to remove the bullet points (because they may be used against you in some fashion in the future), and re-write the requirements. The bullet points should go into the GTB section so that there is less chance for a misinterpretation of reinterpretation that would require the implementation of more than one of the bulleted point in order to meet compliance.</p> <p>2) As written, the requirements listed for TCAs in CIP-003-7(i) for Low Impact assets is a subset of the requirements for high and medium impact included in CIP-010-2 R4. As is or if changed the GTB section should include a statement the low impact requirements are a subset of those for High and Medium.</p>		
Likes	0	
Dislikes	0	
<b>Response</b>		
Thank you for your comments.		

1. The use of the bulleted list is consistent with other currently approved standards. The SDT's intention in using the bulleted list is to provide options to satisfy the parent statement, and the SDT purposely included the ability for the Responsible Entity to use other protection methods, rather than those listed, that more adequately fit the entity's environment.

2. The SDT notes that the requirement allows entities to implement a security program as suggested by your comment and includes the flexibility to develop a single plan for implementing Attachment 1, Section 5, Parts 5.3.1 and 5.3.2.

#### Jason Snodgrass - Georgia Transmission Corporation - 1

<b>Answer</b>	Yes
---------------	-----

<b>Document Name</b>	
----------------------	--

#### Comment

Comments: Both sections 5.1 and 5.2 contain an option of “Other method(s) to mitigate the introduction of malicious code” which grants responsible entities flexibility in choosing alternative methods not included in the list of bulleted items as long as the methods achieve the core security objective outlined in section 5. Therefore, it seems that emphasis is placed on achieving the security objective established by the core of section 5 and the distinction between 5.1 and 5.2 is for the plan to include and cover whom is managing TCAs and not specifically to capture the various options bulleted within the required plan.

As such, GTC believes the bullet point “options” introduces unnecessary prescriptive language and can be removed from the requirements without changing the intent of the requirement whatsoever and the drafting team could simplify with an affirmative ballot. GTC recognizes these options provide contextual ideas of how one could go about achieving the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems and further recommends that they be relocated into the guidelines and technical basis of the standard.

This streamlined revision to section 5 could be simplified for clarity of implementation on the front end and clarity of compliance testing on the audit end as follows:

Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 Method(s) to mitigate the introduction of malicious code for Transient Cyber Asset(s) managed by the Responsible Entity, if any.

5.2 Method(s) to mitigate the introduction of malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any.

5.3 For Removable Media, the use of each of the following:

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

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Likes 0

Dislikes 0

### Response

Thank you for your comment.

The use of the bulleted list is consistent with other currently approved standards. The SDT's intention in using the bulleted list is to provide options to satisfy the parent statement, and the SDT purposely included the ability for the Responsible Entity to use other protection methods, rather than those listed, that more adequately fit the entity's environment.

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

Answer

Yes

Document Name

### Comment

Duke Energy would like to see added clarification within the Guidelines and Technical Basis around the concept of an acceptable review of a 3rd party vendors malware mitigation mechanisms. Currently, in Section 5.2 of Attachment 1, a Responsible Entity is required to "Review" one or a combination of the malware mitigation mechanisms of a 3rd party vendor. Our concern is that it is unclear what constitutes an acceptable "review" of these mechanisms. It is possible that what is considered an acceptable review by one entity, may not be considered acceptable by another. We suggest the drafting team consider adding language to the Guidelines and Technical Basis further describing what constitutes an acceptable review.

Likes 0

Dislikes	0
<b>Response</b>	
Thank you for your comment.	
Specific approaches on how to perform the review could be submitted as Implementation Guidance in accordance with NERC Compliance Guidance Policy.	
<b>Bob Thomas - Illinois Municipal Electric Agency - 4</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.	
Likes	0
Dislikes	0
<b>Response</b>	
Please see the SDT's responses to comments submitted by APPA.	
<b>Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
We like to see examples how to have the ability to restrict malware to the TCA's. Also like to see some examples around technical guidance and mitigation plans. Possibly adding administrative control methods in the technical basis sections for transient devices. Add language in the technical basis restricting movement of TCA's.	
Likes	0
Dislikes	0

**Response**

Thank you for your comment.

The "other" category is intended to allow for future technology or accommodate approaches not considered during the development of the standard. Specific approaches could be submitted as implementation guidance at any point in the future.

**John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1**

<b>Answer</b>	Yes
---------------	-----

<b>Document Name</b>	
----------------------	--

**Comment**

Tacoma Power supports comments submitted by APPA.

In Attachment 1, Section 5, 5.2, what frequency is intended by the words "prior to"? Is this intended to be once upon execution of a vendor/contractor support contract, or is it intended to be at some other interval/frequency?

Likes	0
-------	---

Dislikes	0
----------	---

**Response**

Thank you for your comment.

Per the G&TB for Attachment 1, Section 5, Part 5.2; there is no specific frequency of performance, and the G&TB states "The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code...the SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective."

**Roger Dufresne - Hydro-Qu?bec Production - 5**

<b>Answer</b>	Yes
---------------	-----

<b>Document Name</b>	
----------------------	--

**Comment**

Summary of changes in page 44 of the guidelines CIP010 mentioned :

“All requirements related to TCA and RM are included within a single standard, CIP010. But requirements exist also in CIP-003-07 R2 . HQP suggest to modify the summary of changes.

The word “Managed” should be in lower case for paragraph in the page 56 of 62 “**Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity**”.

It could be usefull to introduce base of risk in the case of a TCA connected to LOW impact BES systems without external connectivity.

Likes 0

Dislikes 0

**Response**

Thank you for your comments.

The SDT includes requirements for TCAs and RM for Lows in CIP-003 to remain consistent with Attachment 1 of CIP-003, which is devoted to protections around Low Impact Assets.

The term "Managed" is capitalized here because the term is part of the title of the section.

Although not required, the proposed requirements allow an entity to assess risk based on external connectivity. Regardless of external connectivity, the SDT asserts that per FERC Order 822, a Responsible Entity must develop a plan around mitigating the risk of introducing malicious code to low impact BES Cyber Systems.

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

**Answer**

Yes

**Document Name**

**Comment**

Summary of changes in page 44 of the guidelines CIP010 mentioned :

“All requirements related to TCA and RM are included within a single standard, CIP010. But requirements exist also in CIP-003-07 R2 . HQP suggest to modify the summary of changes.

The word “Managed” should be in lower case for paragraph in the page 56 of 62 “**Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity**”.

It could be usefull to introduce base of risk in the case of a TCA connected to LOW impact BES systems without external connectivity.

Likes	0
-------	---

Dislikes	0
----------	---

### Response

Thank you for your comments.

The SDT includes requirements for TCAs and RM for Lows in CIP-003 to remain consistent with Attachment 1 of CIP-003, which is devoted to protections around Low Impact Assets.

The term "Managed" is capitalized here because the term is part of the title of the section.

Although not required, the proposed requirements allow an entity to assess risk based on external connectivity. Regardless of external connectivity, the SDT asserts that per FERC Order 822, a Responsible Entity must develop a plan around mitigating the risk of introducing malicious code to low impact BES Cyber Systems.

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

Answer	Yes
--------	-----

Document Name	
---------------	--

### Comment

Santee Cooper agrees with APPA's comments.

Likes	0
-------	---

Dislikes	0
----------	---

Response	
Please see the SDT's responses to comments submitted by APPA.	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Recommend revisions to remove the bulleted list and re-write the requirements. The bullet points should go into the GTB section so that there is less chance for a misinterpretation that would require the implementation of more than one of the bulleted point in order to meet compliance.	
Likes	0
Dislikes	0
Response	
Thank you for your comment.	
The use of the bulleted list is consistent with other currently approved standards. The SDT's intention in using the bulleted list is to provide options to satisfy the parent statement, and the SDT purposely included the ability for the Responsible Entity to use other protection methods, rather than those listed, that more adequately fit the entity's environment.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0

<b>RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Christopher Chavez - Salt River Project - 1,3,5,6 - WECC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Bobby Olsen - Salt River Project - 6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Likes	0
Dislikes	0
<b>Response</b>	
<b>Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1,3</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0

<b>Response</b>	
<b>Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Sean Bodkin - Dominion - Dominion Resources, Inc. - 6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Ryan Olson - Portland General Electric Co. - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	

<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Karie Barczak - DTE Energy - Detroit Edison Company - 3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Stephanie Little - APS - Arizona Public Service Co. - 5</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Patricia Lynch - NRG - NRG Energy, Inc. - 5</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group</b>	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion and OPG</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray</b>	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	

Dislikes 0	
<b>Response</b>	
<b>Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
<p>We continue to 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. This concern continues to fail to be addressed by the SDT. With respect to Attachment 1 Section 3, and Attachment 2, Section 3.1, it doesn't make sense to keep referring to physical location when it comes to electronic controls (as previously noted).</p>	
Likes 0	
Dislikes 0	

**Response**

Thank you for your comments.

The G&TB provides SDTs a mechanism to: (i) explain the technical basis for the associated Reliability Standard (and Requirements therein); and (ii) provide technical guidance to help support effective application of the associated Reliability Standard.

As provided in the response to draft 2 of CIP-003-7, the requirement language does not prescribe a physical versus logical approach to the implementation. The use of the term "asset" refers to assets identified as containing low impact BES Cyber System(s) pursuant to CIP-002. As described in the G&TB, the Responsible Entity has the flexibility to identify the electronic boundary surrounding the low impact BES Cyber System rather than using a physical boundary.

**4. Attachment 2: The SDT revised the evidential language of CIP-003-7(i), Attachment 2, Section 5 to make the Measures consistent with the requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.**

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, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; 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 FMPPA

Answer	No
Document Name	

**Comment**

The complexity of the sentences are difficult to read and understand. Suggest revising to bulleted lists. The evidence requirements seem to require an inventory of TCA's and RM. This could be an issue in the same way that a list of BES Cyber Systems has been determined to be an issue.

Likes 0	
Dislikes 0	

**Response**

While the SDT thanks you for the comment, we decline to make the suggested modification to the format. Although the definition of TCA references BES Cyber Assets (BCA), a discrete list of BCAs or BES Cyber Systems is not required. However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any Removable Media prior to connecting it to a low impact BES Cyber System(s).

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

Answer	No
Document Name	

**Comment**

Reclamation appreciates the Standards Drafting Team's consideration of prior recommendations. Reclamation agrees with the changes and has the following question:

In this version of CIP-003-7(i), did the SDT intend to add guidance regarding the new section on page 9 under Requirement 1 "1.2.6 Declaring and responding to CIP Exceptional Circumstances" in Attachment 1 and/or Attachment 2?

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

The SDT added G&TB language for Requirement R1, Part 1.2.6.

**Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators**

**Answer**

No

**Document Name**

**Comment**

We disagree with the proposed language, as the SDT has only restated the content of the requirement language. There is no process or guidance for an entity to follow when a vendor fails to comply with required request. Is a vendor's attestation sufficient proof for an entity to demonstrate reasonable assurance for compliance? If so, an attestation should be included in the list of acceptable evidence for this requirement, and reflected in Attachment 2 to ensure consistent regional application.

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

The SDT notes that the requirement allows entities the flexibility to develop and implement the plan(s) appropriate for the entity's environment. The evidence that an entity will need to utilize will be dependent on the plan that is in place to mitigate the threat of introduction of malicious code at Lows.

**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 change creates additional requirements for Low Impact BCS relating to change control (additional cost implications from an administrative standpoint with limited reliability benefit) (i.e. capture every time a TCA is connected to a system and this infers that an entity is required to document a discrete list of Cyber Assets for Low Impact BCS)

NRG recommends deleting the quoted portion of the phrase from Section 5 of Attachment 2, number 2: Examples of evidence for Section 5.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures “that document a review of the installed antivirus update level” because it imposes change management requirements where there are not existing NERC requirements

Likes 0

Dislikes 0

**Response**

Thank you for your comments.

The requirement allows the entity to have flexibility in creating a plan to best meet the needs of its organization. This includes the production of compliance evidence.

The list of example evidence within the measure is not a requirement and is not exhaustive.

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

**Answer** No

<b>Document Name</b>	
<b>Comment</b>	
ITC Holdings agrees with the comment submitted by NSRF – see below:	
Please see question 3 for comments concerning “review”. By explaining what the acceptable level of “review” is, the small entity will not be caught in a catch 22. Whereby the “other party” will not state that they meet the attributes of 5.2 and the small entity will have a Low Impact BES Cyber System that cannot be upgraded.	
Likes	0
Dislikes	0
<b>Response</b>	
Please see the SDT’s response to NSRF for Question 3.	
<b>Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Considering the current draft language of the standard, the required evidence can be improved. There is a tradeoff that must be considered between adequate evidence to demonstrate both 1) compliance and assurance that the risk of introduction of malware is mitigated and 2) evidence collection across a large number of sites becoming excessively burdensome. The standard and evidence must be both effective and efficient.	
The expectations for adequate evidence do not fit the audit style currently being used in compliance monitoring. For example, the CIP Version 5 Evidence Request is clearly written to require often extensive documentation of implementation, whereas the measures documented are inconsistent. The measures should be built to provide an example of evidence that would either meet the current evidence request approach or to clearly communicate the intent of the SDT what appropriate evidence would be.	
For Measure 5.1, an example of alternative language to clarify audit expectations would be:	

Examples of evidence for Section 5.1 may include, but are not limited to,

1. Documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code; and
2. Either documentation of an appropriate set of controls that provide a high level of assurance that malware is not present on the Transient Cyber Asset prior to use; or documentation that the Transient Cyber Asset followed the documented method and demonstrates that no identifiable malware is present prior to use.

If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

For Measure 5.3, an example of alternative language that may meet this intent could include:

Examples of evidence for Section 5.3 may include, but are not limited to,

1. Documented process(es) of the method(s) used to detect malicious code; and
2. Either documentation of an appropriate set of controls that provide a high level of assurance that malware is not present on the Removable Media prior to use; or documentation that the Transient Cyber Asset followed the documented method and demonstrates that no identifiable malware is present prior to use.

Likes	0
Dislikes	0

### Response

Thank you for your comments.

The SDT includes examples of evidence it considers valid to meet the requirement. The evidence request is not a product of the SDT. The examples provided in the measures are not intended to be all-inclusive. There are other ways to demonstrate compliance with the requirement that an entity may employ as long as the objective of the requirement is met. The requirement allows the entity to have flexibility in creating a plan to best meet the needs of its organization.

<b>Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
We recommend modifying the first sentence of 5.3.1 to read: “Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code, including an example of the results.” The original language is confusing, and we believe we should avoid the suggestion of a requirement to capture and retain transactional-level evidence as this would be administratively burdensome.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment.	
The SDT asserts that the measure describes the results of scan settings not the scan themselves. Additionally the SDT asserts that the language in a measure is not a requirement. It is up to the entity to determine what would be sufficient evidence of compliance.	
<b>Julie Hall - Entergy - 6</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
CIP-003-7(i), Attachment 2, Section 5, Part 3 is inconsistent with Part 1. Part 3 states that “Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media”. Entergy views the documented process(es) and the results of scanning as two separate pieces of evidence. Part 1 identifies the documented process(es) as an acceptable form of evidence with no requirement for scan results for TCA. Part 3 as written implies that all scans results of applicable Removable Media must be maintained in order to provide proper evidence of compliance with CIP-003-7(i), Attachment 1, Section 5.3. This is in stark contrast to the proposed “Supplemental Material” which states that “the SDT does not intend for a Responsible Entity to conduct a review for every single connection of that Removable Media, but implement their	

process(es) in manner that protects all BES Cyber Systems where the Removable Media may be used. The intent is also not to require a log documenting each connection of Removable Media to a BES Cyber Asset.” Entergy proposes that CIP-003-7(i), Attachment 2, Section 5, Part 3 be rewritten to more closely mirror Part 1 which identifies the documented process as the evidence item. Specific scan results should be identified as potential additional evidence to support Registered Entities programs.

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

The SDT asserts that the measure describes the results of scan settings not the scan themselves. Additionally the SDT asserts that the language in a measure is not a requirement. It is up to the entity to determine what would be sufficient evidence of compliance.

**Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC**

**Answer**

No

**Document Name**

**Comment**

Seattle City Light agrees with the revisions so far as they go, but finds that they do not address the question of what would be acceptable evidence of the existence of any Low impact Removable Media Asset (based on the proposed definition) in the absence of an explicit list of Low impact BES Cyber Systems and Assets at a facility. As discussed in the definition comment above, Seattle does not have a solution to the problem, which is inherent to the structure of CIP version 5/6.

Likes 0

Dislikes 0

**Response**

While the SDT thanks you for the comment, we decline to make the suggested modification to format. Although the definition of TCA references BES Cyber Assets (BCA), a discrete list of BCAs or BES Cyber Systems is not required; However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES Cyber Systems, and must have a plan (in

accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any Removable Media prior to connecting it to a low impact BES Cyber System(s).

**Michael Ward - Seminole Electric Cooperative, Inc. - 4**

**Answer** No

**Document Name**

**Comment**

Same as previous answer.

Likes 0

Dislikes 0

**Response**

Please see the SDT's response to the previous comment.

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

**Answer** No

**Document Name**

**Comment**

We continue to 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. This concern continues to fail to be addressed by the SDT. With respect to Attachment 1 Section 3, and Attachment 2, Section 3.1, it doesn't make sense to keep referring to physical location when it comes to electronic controls (as previously noted).

Likes 0

Dislikes 0

**Response**

Thank you for your comments.

The G&TB provides SDTs a mechanism to: (i) explain the technical basis for the associated Reliability Standard (and Requirements therein); and (ii) provide technical guidance to help support effective application of the associated Reliability Standard.

As provided in the response to draft 2 of CIP-003-7, the requirement language does not prescribe a physical versus logical approach to the implementation. The use of the term "asset" refers to assets identified as containing low impact BES Cyber System(s) pursuant to CIP-002. As described in the G&TB, the Responsible Entity has the flexibility to identify the electronic boundary surrounding the low impact BES Cyber System rather than using a physical boundary.

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

<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Please see question 3 for comments concerning “review”. By explaining what the acceptable level of “review” is, the small entity will not be caught in a catch 22. Whereby the “other party” will not state that they meet the attributes of 5.2 and the small entity will have a Low Impact BES Cyber System that cannot be upgraded.	
Likes	0
Dislikes	0

**Response**

Please see the SDT’s response to Question 3.

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

<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0

Response	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
There is a concern with the requirement that not only requires an inventory of Transient Cyber Assets and Removable Media but it also requires evidence of chain of custody. The SDT needs to provide clarity on what is required for "evidence of chain of custody".	
Likes	0
Dislikes	0
Response	
Thank you for the comment.	
Although the definition of TCA references BES Cyber Assets (BCA), a discrete list of BCAs or BES Cyber Systems is not required. However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any TCA or RM prior to connecting it to a low impact BES Cyber System(s). There is no requirement for "evidence of chain of custody."	
Si Truc Phan - Hydro-Quebec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Section 5.1 in page 32 to 62: To lighten a obligation of maintaining an inventory of TCA of <i>Low impact BES Cyber System</i> , HQP suggest to remove the notion of Trancient asset capability and change the paragraph by " the Responsible Entity or the vendor may document the method used to mitigate the introduction of malicious code"	
Likes	0

Dislikes	0
<b>Response</b>	
Thank you for the comment.	
Although the definition of TCA references BES Cyber Assets (BCA), a discrete list of BCAs or BES Cyber Systems is not required. However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any TCA or RM prior to connecting it to a low impact BES Cyber System(s). Compliance with the requirements is the responsibility of the entity being audited.	
<b>Roger Dufresne - Hydro-Quebec Production - 5</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Section 5.1 in page 32 to 62: To lighten a obligation of maintaining an inventory of TCA of <i>Low impact BES Cyber System</i> , HQP suggest to remove the notion of Transient asset capability and change the paragraph by “ the Responsible Entity or the vendor may document the method used to mitigate the introduction of malicious code”	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for the comment.	
Although the definition of TCA references BES Cyber Assets (BCA), a discrete list of BCAs or BES Cyber Systems is not required. However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any TCA or RM prior to connecting it to a low impact BES Cyber System(s). Compliance with the requirements is the responsibility of the entity being audited.	
<b>John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1</b>	
Answer	Yes

<b>Document Name</b>	
<b>Comment</b>	
Tacoma Power supports comments submitted by APPA.	
Does the Standards Drafting Team intend that any kind of sign-in sheets may be required at assets containing low impact BES Cyber Systems?	
Likes	0
Dislikes	0
<b>Response</b>	
Please see the SDT's responses to comments submitted by APPA.	
<b>Bob Thomas - Illinois Municipal Electric Agency - 4</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.	
Likes	0
Dislikes	0
<b>Response</b>	
Please see the SDT's responses to comments submitted by APPA.	
<b>Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

The complexity of the sentences are difficult to read and understand. Suggest revising to bulleted lists. The evidence requirements seem to require an inventory of TCA's and RM. This could be an issue in the same way that a list of BES Cyber Systems has been determined to be an issue.

Likes 0

Dislikes 0

**Response**

While the SDT thanks you for the comment, we decline to make the suggested modification to format. Although the definition of TCA references BES Cyber Assets (BCA), a discrete list of BCAs or BES Cyber Systems is not required. However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any Removable Media prior to connecting it to a low impact BES Cyber System(s).

**Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov**

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

**Response**

**Glen Farmer - Avista - Avista Corporation - 1,3,5**

Answer

Yes

Document Name

Comment

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Ronald Donahey - TECO - Tampa Electric Co. - 3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion and OPG</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Likes 0	
Dislikes 0	
<b>Response</b>	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Karie Barczak - DTE Energy - Detroit Edison Company - 3</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Stephanie Little - APS - Arizona Public Service Co. - 5</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
<b>Response</b>	
Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jason Snodgrass - Georgia Transmission Corporation - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	

<b>Response</b>	
<b>Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Chris Scanlon - Exelon - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Ryan Olson - Portland General Electric Co. - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	

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

<b>Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1,3</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Bobby Olsen - Salt River Project - 6</b>	
Answer	Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Christopher Chavez - Salt River Project - 1,3,5,6 - WECC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	

<b>Response</b>	
<b>Jamie Monette - Allete - Minnesota Power, Inc. - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Rachel Coyne - Texas Reliability Entity, Inc. - 10</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
Texas RE noticed the following:	
<ul style="list-style-type: none"> <li>• Page 31, Section 1. Cyber Security Awareness; there is an extra “_” that is not needed after the colon symbol.</li> <li>• Page 31, Section 2. Physical Security Controls; there is an extra “_” that is not needed after the colon symbol.</li> <li>• Page 33, Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation; there no period “.” at the end of the first continued paragraph.</li> </ul>	
Likes	0
Dislikes	0

**Response**

Thank you for your comments.

The SDT made the modifications.

**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.**

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

Answer No

Document Name

Comment

We continue to 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. This concern continues to fail to be addressed by the SDT. With respect to Attachment 1 Section 3, and Attachment 2, Section 3.1, it doesn't make sense to keep referring to physical location when it comes to electronic controls (as previously noted).

Likes 0

Dislikes 0

Response

Thank you for your comments.

The G&TB provides SDTs a mechanism to: (i) explain the technical basis for the associated Reliability Standard (and Requirements therein); and (ii) provide technical guidance to help support effective application of the associated Reliability Standard.

As provided in the response to draft 2 of CIP-003-7, the requirement language does not prescribe a physical versus logical approach to the implementation. The use of the term "asset" refers to assets identified as containing low impact BES Cyber System(s) pursuant to CIP-002. As described in the G&TB, the Responsible Entity has the flexibility to identify the electronic boundary surrounding the low impact BES Cyber System rather than using a physical boundary.

**Michael Ward - Seminole Electric Cooperative, Inc. - 4**

<b>Answer</b>	No
---------------	----

<b>Document Name</b>	
----------------------	--

**Comment**

Same as previous answer

Likes	0
-------	---

Dislikes	0
----------	---

**Response**

Please see the SDT's response to your previous comment.

**Julie Hall - Entergy - 6**

<b>Answer</b>	No
---------------	----

<b>Document Name</b>	
----------------------	--

**Comment**

Supplemental Material, Requirement R2, Attachment 1, Section 5.1 – Transient Cyber Asset(s) Managed by the Responsible Entity, Paragraph 4 states that if a device will be used to “For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.” This may imply that at least *some* logs might need to be created for connections of TCA to BCA, which is not a requirement stated in the standard for TCAs at low impact BCS, or even for TCAs at Highs and Mediums under CIP-010-2. Additionally, requiring documentation that a TCA was updated before connecting to a BCA removes the device from the on-going program and puts it into on-demand space due to “has been updated before being connected” implying the device is as up to date as possible, even though the on-going process may allow for devices to be updated on a longer regular interval. If the TCA was truly maintained as part of the entity's on-going program, no additional log or documentation should be required as the device would be compliant with the standard as written.

Supplemental Material, Requirement R2, Attachment 1, Section 5.1 – Transient Cyber Asset(s) Managed by the Responsible Entity, Paragraph 4 Mitigation of the threat of detected malicious code on the Removable

Media prior to connecting Removable Media to a low impact BES Cyber System. Periodicity.

Likes 0

Dislikes 0

**Response**

Thank you for your comments.

Requirement R2 is a plan-based requirement, and evidence to demonstrate compliance is based on content in its plan. The requirement allows the entity to have flexibility in creating a plan to best meet the needs of their organization. This may include the specification of update periodicity. Responsible Entities may review the G&TB, RSAW, and corresponding measure(s) for additional information.

**Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC**

**Answer**

No

**Document Name**

**Comment**

BPA believes that for Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems--entities must manage these assets under the program that matches the highest impact level to which they will connect.

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

This is an example of the why the SDT aligned the language used in the requirements for Transient Cyber Assets used at low impact BES Cyber System(s) and medium/high impact BES Cyber System(s).

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

<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<p>Considering the current draft language of the standard, the GTB addresses the required points. However, the messages are not clearly, simply, and constructively communicated. While the teams have clearly put a considerable amount of work into ensuring each detail is correct, the overall message in the guidance gets lost. This results in opportunities for multiple different interpretations by various entities and auditors.</p> <p>One possible control is testing the operation of antivirus to test signatures. These should be specifically noted that use of test signatures is not considered identified malware.</p> <p>Section 5.2 (and likely all of the guidance) could be improved if the GTB approach was changed to treat malware protection as a program with specific objectives and a selection of example techniques that may be used to meet these objectives. Further, the guidance should be coordinated with the requirements in development by the Supply Chain SDT.</p>	
Likes	0
Dislikes	0
<b>Response</b>	
<p>Thank you for your comments.</p> <p>The obligation specified in the requirement is for entities to implement one or more documented plan(s) for its low impact BES Cyber System(s). The entity has flexibility to determine what methods to include in its plan so long as they meet the security objective to mitigate the risk of the introduction of malicious code into the BES Cyber System through the use of Transient Cyber Assets or Removable Media.</p>	
<b>Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	

ITC does not agree with the proposed modification in regards to guidance provided for awareness training. The revised guidance states "The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel". This statement is ambiguous and leaves the interpretation as to whether or not tracking of reception of awareness training is actually required to maintain compliance. The specific and direct language of "Responsible Entity is not required" should be retained, to reduce confusion and ambiguity as to if this is required for compliance and not left to the disposition of individual auditors. ITC recommends that this specific change be struck and the original language to stand.

All other changes are acceptable.

Likes 0

Dislikes 0

#### Response

Thank you for your comment.

The SDT made the change to reflect that the G&TB does not prescribe what is or is not required to demonstrate compliance.

**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 correction of grammatical / spelling error: on page 57 of 62 of the Guidelines and Technical basis section for requirement 2.

&bull; If a Responsible Entity chooses *to use* methods that mitigate the introduction of malicious code other than those listed, it should *document at* how the other method(s) meet the mitigation of the introduction of malicious code objective.

Pertaining to project 2016-02, NRG recommends that the Low Impact requirements should be incorporated into the existing CIP standards using applicability tables because this would remove inconsistencies and confusion between L/M/H and provide more efficiency within the industry. For example, applied CIP-010-2 Attachment 1 for TCA and Removable Media requirements, with the exception of the authorized user or machine lists.

Likes	0
Dislikes	0
<b>Response</b>	
<p>Thank you for your comments.</p> <p>The SDT has made the suggested changes.</p> <p>While the SDT appreciates the comments regarding the placement of the low impact requirements, we decided to retain the current CIP-003 plan structure due to a majority of stakeholder support.</p>	
<b>Wendy Center - U.S. Bureau of Reclamation - 5</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
<p>Reclamation appreciates the Standards Drafting Team's consideration of prior recommendations. Reclamation agrees with the changes and has the following comment:</p> <p>In the redline version of the Guidelines and Technical Basis, some typographical errors include:</p> <ul style="list-style-type: none"> <li>• The spelling of "Responsible Entities" on the sixth line of page 55.</li> <li>• A duplicate paragraph at the bottom of page 56 and the top of page 57.</li> <li>• The spelling of "to use" and "document" in the third bullet of page 57.</li> <li>• The word "is" at the beginning of a sentence on the third line from the bottom of page 57.</li> </ul>	
Likes	0
Dislikes	0

<b>Response</b>	
Thank you for your comment.	
The SDT made the suggested modification.	
<b>Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
The information in the GTB section does not appear to be consistent with the information in Requirement R2. Our interpretation of Requirement R2 suggests that there is not enough clarity in the Requirement to differentiate whether the focus is solely on CIP-002 and its attachment 1 or is the focus more on CIP-003-7(i) and its Attachment 1. We suggest adding clarity to the Requirement and/or the GTB to ensure that there is no confusion as to the Requirement’s intent as well as what an audit team’s interpretation of the performance of an entity during the auditing process.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment.	
Where Attachment 1 or Attachment 2 is specified within the standard without explicit reference to another standard, the attachment pertains to the standard wherein the reference was made. No change made.	
<b>Patricia Lynch - NRG - NRG Energy, Inc. - 5</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	

Likes	0
Dislikes	0
<b>Response</b>	
<b>Jamie Monette - Allete - Minnesota Power, Inc. - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes. To avoid confusion with CIP-010 R1 requirements, we suggest the removal of "change management process" in the prior sentence.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment.	
The SDT agrees that there is no obligation for entities to implement a change management process for low impact BES Cyber System(s), although entities may have such processes. The G&TB does not and cannot introduce any obligations that are not specified in the requirement language.	
<b>Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Seattle City Light appreciates the extra efforts of the Standard Drafting Team to provide such guidance and technical information. However, Seattle asks that Guidelines and Technical Basis information be provided for new Section 1.2.6 as well. This guidance would	

address how a CIP Exceptional Circumstance is considered when applied against a requirement that does not explicitly mention that a CIP Exceptional Circumstance applies.

Likes 0

Dislikes 0

### Response

Thank you for your comment.

The SDT agrees that providing guidance on the low impact policy is beneficial and has made such modifications to the G&TB. However, the SDT notes that - unless explicitly stated - CEC does not apply.

**Shannon Fair - Colorado Springs Utilities - 6, Group Name** Colorado Springs Utilities

**Answer**

Yes

**Document Name**

### Comment

1) The guidance should be coordinated with the Supply Chain SDT.

2) The GTB language that states: "Section 5.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed." is to prescriptive. Recommend that the "are to" be changed to "may". The use of prescriptive language like "should" and "are to" should be used on a very limited basis if not removed entirely. Guidance should be shifted to a programmatic approach.

Likes 0

Dislikes 0

### Response

Thank you for your comments.

The Project 2016-02 Modifications to CIP Standards SDT is coordinating with the Supply Chain SDT as necessary.

The SDT updated the G&TB to more closely align with the requirement language. The intent is to reiterate the need to document and implement the plan as specified in the requirement, not to infer other obligations in the G&TB.

**Bob Thomas - Illinois Municipal Electric Agency - 4**

**Answer** Yes

**Document Name**

**Comment**

Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.

Likes 0

Dislikes 0

**Response**

Please see the SDT’s responses to comments submitted by APPA.

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

**Answer** Yes

**Document Name**

**Comment**

Page 56 of the Guidelines and Technical Basis includes a section titled “Vulnerability Mitigation”; however, Requirement R2, Attachment 1, Section 5 is titled “...Risk Mitigation”. AZPS requests clarification and consistency regarding the terms vulnerability and risk as one term is more subjective than the other.

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

The SDT updated this section of the G&TB to more closely align with the language used in Attachment 1.

<b>John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Tacoma Power supports comments submitted by APPA.	
Likes	0
Dislikes	0
<b>Response</b>	
Please see the SDT's responses to comments submitted by APPA.	
<b>Roger Dufresne - Hydro-Qu?bec Production - 5</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
No comments for section 5.	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
None.	

Likes	0
Dislikes	0
<b>Response</b>	
<b>Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion and OPG</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Two comments.	
First, recommend changing “should” to “may” in this paragraph	
To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.1 Procurement language may unify the other party’s and entity’s actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party’s support. Entities should consider the “General Cybersecurity Procurement Language” and “The Supplier’s Life Cycle Security Program” when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.	
Second, recommend updating 5.3 from “If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System.” to “If malicious code is discovered, it must be removed or mitigated prior to connection to a BES Cyber Asset or BES Cyber Systems in order to prevent the malicious code from being introduced into the BES Cyber Asset or BES Cyber System.”	
Likes	0
Dislikes	0

**Response**

Thank you for your comments.

The SDT modified the G&TB accordingly.

**Ronald Donahey - TECO - Tampa Electric Co. - 3**

**Answer** Yes

**Document Name**

**Comment**

The guidance should be coordinated with the Supply Chain SDT.

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

The Project 2016-02 Modifications to CIP Standards SDT is coordinating with the Supply Chain SDT as necessary.

**RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC**

**Answer** Yes

**Document Name**

**Comment**

Likes 0

Dislikes 0

**Response**

<b>Christopher Chavez - Salt River Project - 1,3,5,6 - WECC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Bobby Olsen - Salt River Project - 6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1,3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Likes	0
Dislikes	0
<b>Response</b>	
<p><b>Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino</b></p>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<p><b>Karie Barczak - DTE Energy - Detroit Edison Company - 3</b></p>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	

<b>Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Sean Bodkin - Dominion - Dominion Resources, Inc. - 6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Ryan Olson - Portland General Electric Co. - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Chris Scanlon - Exelon - 1</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Jason Snodgrass - Georgia Transmission Corporation - 1</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF</b>	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>David Gordon - Massachusetts Municipal Wholesale Electric Company - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators</b>	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	

Dislikes	0
<b>Response</b>	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes

<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Glen Farmer - Avista - Avista Corporation - 1,3,5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	

Dislikes	0
<b>Response</b>	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
<b>Comment</b>	
Texas RE noticed the following:	
<ul style="list-style-type: none"> <li>• Page 56, Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity states, <i>“For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.”</i> Since this concept is the same as described in the Guidelines and Technical Basis of CIP-005-5, Texas Re suggests that the SDT use the same “high water mark” language found in the Guidelines and Technical basis of CIP-005-5 to stay consistent.</li> <li>• Page 57, Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity states, <i>“The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.”</i> Texas RE considers keeping a list of BES Cyber Assets as best practice and this language discourages it. Texas RE encourages entities to have an inventory of their low impact BES Cyber Systems.</li> <li>• Page 57, Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity states, <i>“If a Responsible Entity chooses touse methods...”</i> There should be a space between “touse”.</li> </ul>	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comments.	

The SDT asserts that the language is sufficiently clear in the G&TB to describe the necessary treatment of Transient Cyber Assets.

Requirement R2 is a plan-based requirement, and evidence to demonstrate compliance is based on the content in the entity’s plan(s). While an entity may comply with the requirement by creating an inventory, the G&TB is accurate in conveying that the intent of the SDT was not to create such an obligation.

The SDT made the modification.

**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, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; 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 FMPPA**

Answer

Document Name

Comment

1) The guidance should be coordinated with the Supply Chain SDT.

2) The GTB language that states: “Section 5.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.” is to prescriptive. Recommend that the “are to” be changed to “may”. The use of prescriptive language like “should” and “are to” should be used on a very limited basis if not removed entirely. Guidance should be shifted to a programmatic approach.

Likes 0

Dislikes 0

**Response**

Thank you for your comments.

The Project 2016-02 Modifications to CIP Standards SDT is coordinating with the Supply Chain SDT as necessary.

The SDT updated the G&TB to more closely align with the requirement language. The intent is to reiterate the need to document and implement the plan as specified in the requirement, not to infer other obligations in the G&TB.

**6. Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the standard, 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. Were the CEC language is explicitly stated, entities need not**

**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.

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

The RSAW is not a product of the SDT.

**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**

Pertaining to project 2016-02, CIP-003-7(i), it doesn't appear that the implementation plan accounts for additional time to implement 1.2.5 and 1.2.6. NRG recommends that the implementation plan allow for 18 months implementation time of 1.2.5 and 1.2.6. (the same implementation time as other requirements)

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

The implementation plan specifies that CIP-003-7(i) will become effective 18 months following applicable regulatory approval. This is inclusive of the modifications to Requirement R1.

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

Answer

No

Document Name

**Comment**

ITC Holdings agrees with the comments compiled by the EEI CIP Standards subgroup– see below:

SUMMARY:

CIP-003-6, Requirement R2, Attachment 1, sections 2 and 3 have been approved (under the Order No. 822 implementation plan) to be effective on September 1, 2018. However, in Order No. 822, the Commission ordered NERC (within 1 year) to provide clarity regarding the LERC (Low Impact External Routable Connectivity) definition, specifically ambiguity surrounding the term "direct" used in the definition. When the SDT set out to modify the definition they found that it was more appropriate to modify the requirement language to address the ambiguity. The modified standard (version 7) is expected to be filed with FERC by March 31, 2017.

CIP-003-6, Requirement R2, Attachment 1, sections 2 and 3 is effective September 1, 2018 and version 7, if FERC approves, will be effective 18 months from FERC's approval, so doing rough math (March 31, 2017 NERC filing of version 7, August 2017 NOPR--assuming

~5 months FERC review, February 2018 FERC approval--assuming 60 day notice and comment, and 3 month FERC review): version 7 would become effective around August 2019, basically a year after Version 6 (the time it took NERC to make the modification).

**RATIONALE:**

Reasons for supporting a change to the implementation plan: 1) retiring the implementation of CIP-003-6, attachment 1, sections 2 and 3; 2) syncing up the implementation the low impact BES Cyber System modifications (attachment 1, sections 2, 3, and 5); and 3) giving entities 18 months to implement these sections:

1. Companies will not have certainty regarding CIP-003-6 implementation until February 2018, but will have to move forward on version 6 to make the Sept. 2018 compliance deadline or accept the compliance risk by not implementing version 6.
2. According to the Commission (Order No. 822), the CIP-003-6 modification "is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition." As a result, implementation of CIP-003-6 without the modification doesn't make much sense in light of the ambiguity identified by the Commission.
3. Low impact BES Cyber Systems (LIBCS) have a low impact to the BES compared to medium and high impact BES Cyber Systems.
4. LIBICS number in the tens of thousands systems; it will take time to carefully implement the new CIP-003 requirements. Implementing CIP-003-6 LERC, CIP-003-7 LERC, and then CIP-003-7 TCA in three steps will strain resources for systems with low impact to the BES. It would be more efficient to implement just the CIP-003-7 LERC and TCA modifications at the same time.
5. Change management at this scale, will also be more effective if done all at once, which will help reduce the potential spike in audit violations.

Likes 0

Dislikes 0

**Response**

Thank you for your comments.

The SDT agrees that it is important to align the initial implementation of Sections 2, 3 and 5 of Attachment 1. The effective dates or phased-in compliance dates within the CIP-003-6 Implementation Plan, remain in effect except that the compliance dates for CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3 shall be replaced with the effective date of CIP-003-7.

<b>Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
While achievable in 18 calendar months, the standard needs significant improvement before a yes vote on the implementation.	
Likes	0
Dislikes	0
<b>Response</b>	
Please see the SDT's responses to the subject comments.	
<b>Julie Hall - Entergy - 6</b>	
<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Entergy cannot agree with the Implementation Plan timeline given the standard as written, and the concerns discussed in the comments submitted above. Until clarity is given regarding the scope and evidentiary requirements necessary to achieve compliance, Entergy cannot support the short implementation timeline proposed as the feasibility of implementing controls and evidentiary requirements to meet the standard as currently drafted in that small timeframe for an Entity as large as Entergy is miniscule.	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment.	
The SDT asserts that the 18 month implementation period is sufficient for entities to implement the standards.	
<b>Patricia Lynch - NRG - NRG Energy, Inc. - 5</b>	

<b>Answer</b>	No
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
<p>The majority of actions necessitating the timeframe proposed in the Implementation Plan modifications involve identifying and implementing the physical, electronic, and TCA/RM controls necessary for over 1200 assets containing Low Impact BES Cyber Systems, as well as training a massive amount of personnel on meeting and maintaining compliance with these new Standard requirements. Although the requirements themselves may be less rigid than those for Highs and Mediums, the proposed implementation timeframe is required from a volume standpoint, as well as from a risk-based standpoint so as not to divert attention and resources away from meeting and maintaining compliance on all of the other High and Medium risk assets</p>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper</b>	
<b>Answer</b>	Yes

<b>Document Name</b>	
<b>Comment</b>	
None.	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
<p>We strongly support the Implementation Plan, which seeks to replace compliance with CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3 with compliance with CIP-003-7(i) (and CIP-003-7) such that only one implementation is required for the LIBICS modifications, 18 months from FERC approval. Our members agree with the SDT’s approach and offer further explanations as to the importance of this implementation plan:</p>	
<ol style="list-style-type: none"> <li>For CIP-003 alone, EEI members are looking at 3 implementation phases for a very large group of disaggregate assets (substations with variations among systems, types, shared footprints and components as well as generating stations that are extremely complex with many different systems and manufacturers involved). LIBCS number in the tens of thousands of systems; it will take time to carefully implement the new CIP-003 requirements. Implementing CIP-003-6 LERC, CIP-003-7 LERC, and then CIP-003-7 TCA in three steps will strain resources for systems with low impact to the BES.</li> <li>Change management at this scale, will also be more effective if done all at once, which will help reduce the potential spike in audit violations. When we say more effective, we really mean doing it right for security and reliability. Training on one change for CIP-003-6 and then training again for CIP-003-7 will create confusion for field forces. Having one date to train on this culture change management would be more effective when an entity needs to train 250 plus field and engineering people regarding 550 or more low impact BES Cyber</li> </ol>	

Systems. If field people are confused, they will make or may be prone to make mistakes due to confusion or rapidly changing expectations. Potential violations will not protect against security threats or reliability issues.

3. Shared facilities create another implementation issue. For example, an EEI member has approximately half of their low impact substations owned by third parties, shared facilities. To make each of the section 2 and 3 changes, they will have to physically go to each substation, which are owned by different entities and as a result are all different. As a result, the approaches they take at each facility must be different, which is also a good thing in the security world. Eighteen months is necessary to make these changes.
4. The revised CIP-003-7 language including retirement of the LERC definition improves the clarity of the requirements. However, the revisions represent a change in assessment approach and will precipitate a new analysis of which locations will be in scope for section 3. The LERC definition provided a filter by the use of the word 'direct' that could be applied when determining which locations were in scope. The retirement of LERC removed that filter. The new language replacing the LERC definition established new assessment criteria and applies it regardless of direct or indirect connectivity. The change to LERC requires Responsible Entities to perform a new analysis of each of their locations. Applying the CIP-003-7 requirements means that entities must walk down each location in scope to determine the specific configurations (physical and electronic) that exist at the location. These walk downs are currently underway to apply a -6 implementation focused on the definition of LERC from CIP-003-6. The scope of analysis will change under CIP-003-7, so that all locations must be assessed for connectivity and then assessed against the new criteria.

Likes 0

Dislikes 0

**Response**

**Roger Dufresne - Hydro-Quebec Production - 5**

**Answer**

Yes

**Document Name**

**Comment**

No comments for section 6.

Likes 0

Dislikes 0

<b>Response</b>	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
<b>Comment</b>	
CenterPoint Energy agrees with EEI's comments regarding the implementation plan for the Low Impact BES Cyber System modifications.	
Likes	0
Dislikes	0
<b>Response</b>	
Please see the SDT's responses to comments submitted by EEI.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
<b>Comment</b>	
Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.	
Likes	0
Dislikes	0
<b>Response</b>	
Please see the SDT's responses to comments submitted by APPA.	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	

Comment	
Duke Energy agrees with the comments submitted by EEI regarding the proposed Implementation Plan.	
Likes	0
Dislikes	0
Response	
Please see the SDT's responses to comments submitted by EEI.	
<b>Shannon Fair - Colorado Springs Utilities - 6, Group Name</b> Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
None	
Likes	0
Dislikes	0
Response	
<b>Brenda Hampton - Luminant - Luminant Energy - 6, Group Name</b> Luminant	
Answer	Yes
Document Name	
Comment	
Companies with a large number of low impact assets will need this time to educate users about handling TCAs and Removable Media. These assets are categorized as low impact because they inherently have a low ability to negatively impact the Bulk Electric System. We do not want to focus our resources on rolling out this education at the expense of efforts that mitigate risks to assets that inherently have a greater ability to negatively impact the Bulk Electric System.	

During the 18-month implementation plan, we will design the overall processes taking into consideration differences between different plant types (gas, lignite, combustion turbine and combined cycle). We will roll out that program to a single pilot plant to identify lessons learned and improve the experience as we onboard subsequent plants. We anticipate spending 3-5 months to design the processes and pilot the program. The remaining months will be spent rolling out to our fleet (40 units at 15 plants). The 18-month implementation plan is appropriate as it allows us to carefully and thoughtfully assign resources to most effectively and efficiently mitigate cyber risk.

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

**Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov**

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

**Response**

**Glen Farmer - Avista - Avista Corporation - 1,3,5**

Answer

Yes

Document Name

Comment

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Ronald Donahey - TECO - Tampa Electric Co. - 3</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray</b>	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC no Dominion and OPG</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>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, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; 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</b>	
Answer	Yes
Document Name	

<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Wendy Center - U.S. Bureau of Reclamation - 5</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Si Truc Phan - Hydro-Quebec TransEnergie - 1 - NPCC</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>David Gordon - Massachusetts Municipal Wholesale Electric Company - 5</b>	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Karie Barczak - DTE Energy - Detroit Edison Company - 3</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Stephanie Little - APS - Arizona Public Service Co. - 5</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Jason Snodgrass - Georgia Transmission Corporation - 1</b>	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Chris Scanlon - Exelon - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Ryan Olson - Portland General Electric Co. - 5</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC</b>	

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

Dislikes	0
<b>Response</b>	
<b>Michael Ward - Seminole Electric Cooperative, Inc. - 4</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino</b>	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	

<b>Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 5</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1,3</b>	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
<b>Bobby Olsen - Salt River Project - 6</b>	
Answer	Yes
Document Name	
Comment	

Likes	0
Dislikes	0
<b>Response</b>	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
Christopher Chavez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
<b>Comment</b>	
Likes	0
Dislikes	0
<b>Response</b>	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	

<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jamie Monette - Allete - Minnesota Power, Inc. - 1</b>	
<b>Answer</b>	Yes
<b>Document Name</b>	
<b>Comment</b>	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Rachel Coyne - Texas Reliability Entity, Inc. - 10</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
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**

Thank you for your comment.

**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**

Small entities will not be able to go up against a vendor (i. e. Micro Soft in size) and request to review their most current protections to comply with section 5.2. The above clarity will assure we meet the attributes of 5.2. The NSRF does not wish for CIP-003-7(i) to be the number one non compliance Standard going forward in NERC, similar to CIP-007-6.

Likes 0

Dislikes 0

**Response**

Thank you for your comment.

Please see the SDT's response to Question 4.

**Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino**

**Answer**

**Document Name**

**Comment**

Entities are increasing their use of malicious code mitigation using tools such as Cylance, which does not rely on signatures or updates. The measures should consider these tools and provide examples of evidence that will prove compliance.

Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment.	
The SDT contends that your concern is addressed in the last bullet of Attachment 1, Section 5, Part 5.2 that allows entities the flexibility to use “other method(s) to mitigate the introduction of malicious code.” Measures provide examples of evidence and are not intended to be comprehensive lists. Each entity has to decide and provide whatever evidence it determines best demonstrates compliance with any requirement.	
<b>Karie Barczak - DTE Energy - Detroit Edison Company - 3</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
none	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Sean Bodkin - Dominion - Dominion Resources, Inc. - 6</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	

Dominion recommends that the first VSL conditional statement for Requirement 1 Part 1.2 (page 14 of 62 of draft 1 of CIP-003-7(i)) be consistent with the prior version of CIP-003 and read as follows:

Lower VSL: The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two or fewer of the six topics required by R1. (R1.2)

Moderate VSL: The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the six topics required by R1. (R1.2)

High VSL: The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four of the six topics required by R1. (R1.2)

Severe VSL: The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address five or more of the six topics required by R1. (R1.2)

The revised VSLs accurately reflect the actual severity when a failure to address the appropriate topics occurs.

Likes	0
-------	---

Dislikes	0
----------	---

**Response**

Thank you for your comment.

The SDT notes that the current VSL structure is in alignment with CIP-003-6, CIP-003-7, and the informal posting of CIP-003-7(i).

**Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC**

<b>Answer</b>	
---------------	--

<b>Document Name</b>	
----------------------	--

**Comment**

Seattle City Light has additional concerns that led it to vote NO for this ballot. One concern is about new sub-part 1.2.6, which introduces CIP Expectational Circumstances to Low impact facilities. The other concern is about seeming errors in the Violation Severity Level (VSL) tables for some of the new parts and sections introduced in CIP-003-7(i).

Regarding sub-part 1.2.6, Seattle supports the concept of allowing CIP Exception Circumstances for Low impact facilities and related requirements, and find this idea highly sensible and reasonable. Seattle is concerned, however, that the change appeared without notice or discussion in the present draft of CIP-003-7(i), and that the application of CIP Exceptional Circumstances for Lows is not at all defined. In particular, other Standards, parts, and sub-parts of CIP version 5/6 explicitly identify where CIP Exceptional Circumstances are allowed. This explicit mention creates the presumption that CIP Exceptional Circumstances are allowed only for said Standards, parts, or sub-parts; some auditors have stated as such. Seattle is aware that a drafting team effort is planned to address inconsistencies in the existing application of CIP Exceptional Circumstances, and finds it premature to expand the use of CIP Exceptional Circumstances in a way that introduces even more uncertainty—how are they applied to Lows where no existing Low Standard mentions that CIP Exceptional Circumstances are allowed—before the existing issues are addressed. That the concept was introduced without discussion or technical guidance language only heightens our concern. As a possible corrective, Seattle recommends that the Part R2 of CIP-003-7(i) be modified as follows (BOLD text is new):

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall, **EXCEPT FOR CIP EXCEPTIONAL CIRCUMSTANCES**, implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.

Regarding the VSL tables, Seattle does not understand the difference among the Lower, Moderate, and High VSLs for failure to perform some or all of the activities according for Requirement R2, Attachment 1, Section 5.1. For Transient Cyber Assets, the Lower VSL states:

The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2)

The applicable Moderate VSL states:

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. (R2)

And the applicable High VSL reads:

The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2)

Seattle does not understand the difference among the three items, given that the failure to manage according to plan (the Lower VSL) means that introduction of mitigation code is not documented (the Moderate VSL) and/or mitigated (High VSL); there are not other applicable activities to fail. As such, Seattle recommends these be consolidated into a single VSL at the Moderate (or perhaps High) level.

Finally, Seattle also finds confusing the wording in the Lower VSL for Removable Media. For Transient Cyber Assets this VSL states:

The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)

Seattle does not understand how an entity can ever meet the Lower VSL for Removable Media, in that to do so it must “document its plan(s) for...Removable Media but fail to document the Removable Media section(s) according to Requirement 2.” As best as we understand, the Removable Media Plans are the Removable Media sections of Requirement 2, so the statement appears to be in error. As a corrective, Seattle suggests that the Lower VSL entry for Removable Media be modified to mirror that of Transient Cyber Assets, and thus read (BOLD indicates where “Removable Media” was substituted for Transient Cyber Asset):

The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its REMOVABLE MEDIA according to Requirement R2, Attachment 1, Section 5.1. (R2)

Likes	0
Dislikes	0

### Response

Thank you for your comments.

Due to the requirement to perform actions at the time of use of a TCA or RM, an entity may not be able to perform the controls prescribed under Section 5 during a CEC. Therefore, the CEC language was added to address this situation. The other sections under Attachment 1 do not have the same timing aspects as Section 5. The SDT will be seeking industry feedback on the applicability of CEC to other requirements and parts. Requirement 1.2.6 was added to ensure a policy for CEC in the use of TCA and RM. Requirement 1.2.6 was

added to ensure a policy for CEC in the use of TCA and RM. Guidance was added for policy section 1.2.6 on declaring and responding to CEC.

The difference related to TCAs are as follows, the Lower VSL addresses the documentation and management aspects of the requirement. The entity documented its plan but did not follow the plan in managing its TCAs under Section 5.1.

The Moderate VSL addresses the situation where the entity documented their plan, mitigated discovered malicious code, but failed to document the mitigation.

The High VSL addresses where the entity failed to mitigate the introduction of malicious code.

Regarding the Lower VSL for Removable Media, the SDT has revised the VSL to state: The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)

**Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC**

Answer

Document Name

Comment

BPA respectfully suggests spellchecking the redline before finalizing. For example:

Page 33: Entiteis

Page 57: Transiet

Likes 0

Dislikes 0

Response

Thank you for your comment.

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

<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
None	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
<p>1) The word “and” should be added at the end of R1.2.5</p> <p>2) This comment form did not reference the addition of CIP Exceptional Circumstances as Requirement R1.2.6 and the inclusion of the phrase “except under CIP Exceptional Circumstances” in Attachment 1, Section 5. The “except under CIP Exceptional Circumstances” phrase should also be addressed in Attachment 1 Sections 2 and 3. Not addressing CEC in Sections 2 and 3 may result in a “no” vote for on future ballot of this standard.</p> <p>3) A Section 6 under Attachment 2 is needed to explain how the CIP Exceptional Circumstance is to be used so you can put it into your policy/plan accordingly.</p>	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comments.	

The word "and" was added to Requirement R1, Part 1.2.5.

Due to the requirement to perform actions at the time of use of a TCA or RM, an entity may not be able to perform the controls prescribed under Section 5 during a CEC. Therefore, the CEC language was added to address this situation. The other sections under Attachment 1 do not have the same timing aspects as Section 5. The SDT will be seeking industry feedback on the applicability of CEC to other requirements and parts. Requirement 1.2.6 was added to ensure a policy for CEC in the use of TCA and RM. Guidance was added for policy section 1.2.6 on declaring and responding to CEC.

**Bob Thomas - Illinois Municipal Electric Agency - 4**

Answer

Document Name

**Comment**

Illinois Municipal Electric Agency supports comments provided by the American Public Power Association.

Likes 0

Dislikes 0

**Response**

Please see the SDT's responses to comments submitted by APPA.

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

Answer

Document Name

**Comment**

ITC Holdings agrees with the comment submitted by NSRF – see below:

Small entities will not be able to go up against a vendor (i. e. Micro Soft in size) and request to review their most current protections to comply with section 5.2. The above clarity will assure we meet the attributes of 5.2. The NSRF does not wish for CIP-003-7(i) to be the number one non compliance Standard going forward in NERC, similar to CIP-007-6.

Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment.	
Please see the SDT's response to Question 4.	
<b>Aaron Austin - AEP - 1,3,5,6 - SPP RE,RF</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
None	
Likes 0	
Dislikes 0	
<b>Response</b>	
<b>Jeffrey DePriest - DTE Energy - Detroit Edison Company - 5</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
None	
Likes 0	
Dislikes 0	
<b>Response</b>	

<b>Brian Van Gheem - ACES Power Marketing - 6 - NA - Not Applicable, Group Name ACES Standards Collaborators</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
<ol style="list-style-type: none"> <li>1. The inclusion of CIP Exceptional Circumstance for lows adds additional compliance burden above and beyond the FERC Directives. This will require Cyber Security Policy revisions, training and increase audit risk for lows who have not seen any addtional risks to the BES to require CIP Exceptional Circumstances as part of their CIP cyber Security Program.</li> <li>2. If a low impact entity connects an identified 30-day TCA beyond the thirty days, what is the classification of the asset? If this was a high or medium impact entity, the TCA would be classified as a Protected Cyber Asset (PCA). However, PCAs are not applicable to low impact entities, as a low impact's TCA would not be classified as a BES Cyber Asset that could impact the BES within 15 minutes. Would the low impact entity who failed to connect the TCA within the thirty day timeframe have to self-report the TCA to Regional Entities? If so, this would impose a greater violation risk for lows than for high and medium impact entities.</li> <li>3. We thank the SDT for this opportunity to provide comments.</li> </ol>	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comments.	
<ol style="list-style-type: none"> <li>1. An entity is not obligated to use TCAs or RM. The inclusion of CEC for lows was added due to the requirement to perform actions at the time of use of a TCA or RM. An entity may not be able to perform the controls prescribed under Section 5 during a CEC. Therefore, the CEC language was added to address this situation.</li> <li>2. The TCA connected for more than 30 days could be considered a BES Cyber System or a non-BES Cyber System, depending on the facts and circumstances. The handling of this situation could be addressed within the entity's plan.</li> </ol>	
<b>John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1</b>	
<b>Answer</b>	

<b>Document Name</b>	
<b>Comment</b>	
Tacoma Power supports comments submitted by APPA.	
Likes	0
Dislikes	0
<b>Response</b>	
Please see the SDT's responses to comments submitted by APPA.	
<b>Roger Dufresne - Hydro-Quebec Production - 5</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
No comments for section 7.	
Likes	0
Dislikes	0
<b>Response</b>	
<b>Si Truc Phan - Hydro-Quebec TransEnergie - 1 - NPCC</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
Some typos:	
P 55: 'entiteis'	
P 70 of 75: "touse"; ". is the SDT"; "toTransiet Cyber Assets"	

Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment.	
The SDT made the modifications.	
<b>Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
Xcel Energy supports the comments of the Edison Electric Institute.	
Likes	0
Dislikes	0
<b>Response</b>	
Please see the SDT's responses to comments submitted by EEI.	
<b>Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
The CIP Exceptional Circumstance concept does not belong with the Low Impact requirements. The purpose of CIP-007-3i was to define and create requirements for Transient Cyber Assets and Removable Media. The need for Exceptional Circumstances for High and Medium is because the Standard mandates a PRA for unescorted access. Even with Exceptional Circumstances you have to report a violation because of the externally mandated PRA. In the case of Low Impact, the entity writes the requirements for access. Most departments responsible for physical security automatically allow the entrance of Emergency Personnel and Police if there is an alarm or	

911 call. This could be written into each Responsible Entity's Low Impact Cyber Security Policy (CIP-003 R1.2) but that doesn't seem to support BES Reliability.

Likes 0

Dislikes 0

### Response

Thank you for your comments.

Due to the requirement to perform actions at the time of use of a TCA or RM, an entity may not be able to perform the controls prescribed under Section 5 during a CEC. Therefore, the CEC language was added to address this situation. The other sections under Attachment 1 do not have the same timing aspects as Section 5. The SDT will be seeking industry feedback on the applicability of CEC to other requirements and parts.

**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 to 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**

Thank you for your comments.

1. Regarding the Lower VSL for Removable Media, the SDT revised the VSL to state: The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)

2. First VSL related to Requirement R2, Attachment 1, Section 5.3 under Moderate addresses the situation where the entity documented their plan, mitigated discovered malicious code, but failed to document the mitigation. The second VSL related to Requirement R2, Attachment 1, Section 5.3 addresses the situation where the entity failed to implement the Removable Media sections.

**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, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; 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

Document Name

**Comment**

1) The word “and” should be added at the end of R1.2.5

2) This comment form did not reference the addition of CIP Exceptional Circumstances as Requirement R1.2.6 and the inclusion of the phrase “except under CIP Exceptional Circumstances” in Attachment 1, Section 5. The “except under CIP Exceptional Circumstances” phrase should also be addressed in Attachment 1 Sections 2 and 3. Not addressing CEC in Sections 2 and 3 may result in a “no” vote for on future ballot of this standard.

3) A Section 6 under Attachment 2 is needed to explain how the CIP Exceptional Circumstance is to be used so you can put it into your policy/plan accordingly.

Likes 0

Dislikes 0

**Response**

Thank you for your comments.

The word "and" was added to Requirement R1, Part 1.2.5.

Due to the requirement to perform actions at the time of use of a TCA or RM, an entity may not be able to perform the controls prescribed under Section 5 during a CEC. Therefore, the CEC language was added to address this situation. The other sections under Attachment 1 do not have the same timing aspects as Section 5. The SDT will be seeking industry feedback on the applicability of CEC to other requirements and parts. Requirement 1.2.6 was added to ensure a policy for CEC in the use of TCA and RM. Guidance was added for policy section 1.2.6 on declaring and responding to CEC.

**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
<b>Response</b>	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	
Document Name	
<b>Comment</b>	
<p>To address the changes to the RSAW provided on January 20th Under the Note to Auditor section, Attachment 1, Section 3:</p> <p>Bullet 1: Recommended to state that “the devices used to control electronic access” can be documented at a representative level. The standard (Attachment 1, Section 3, Bullet 1) under examples of evidence state that documentation can be “at each asset or group of assets containing low impact BES Cyber Systems” level and can be representative diagrams, meaning a list of devices at each asset is not required under the standard and puts additional documentation burden on the Entity as currently worded in the RSAW.</p> <p>Bullet 2: Recommended to document necessary inbound and outbound routable protocols communications at a standard level versus at each asset (e.g. document SCADA communications as necessary inbound and outbound for the Entities entire system, rather than having to document at each asset) for same reason as our comment for Bullet 1.</p> <p>Bullet 3 and 4: Recommended to document that the electronic access controls can be provided at a standard level (e.g. standard configurations) which would apply to the standard devices, versus providing per asset.</p>	
Likes	0
Dislikes	0
<b>Response</b>	
Thank you for your comment.	
The SDT provided your comments regarding the RSAW to NERC staff for review.	
<b>Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6</b>	

<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
PacifiCorp supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Please see the SDT's responses to comments submitted by EEI.	
<b>Ronald Donahey - TECO - Tampa Electric Co. - 3</b>	
<b>Answer</b>	
<b>Document Name</b>	
<b>Comment</b>	
1) This comment form did not reference the addition of CIP Exceptional Circumstances as Requirement R1.2.6 and the inclusion of the phrase "except under CIP Exceptional Circumstances" in Attachment 1, Section 5. The "except under CIP Exceptional Circumstances" phrase should also be addressed in Attachment 1 Sections 2 and 3.	
Likes 0	
Dislikes 0	
<b>Response</b>	
Thank you for your comment.	
Due to the requirement to perform actions at the time of use of a TCA or RM, an entity may not be able to perform the controls prescribed under Section 5 during a CEC. Therefore, the CEC language was added to address this situation. The other sections under Attachment 1 do not have the same timing aspects as Section 5. The SDT will be seeking industry feedback on the applicability of CEC to other requirements and parts.	



**Additional comments received from American Public Power Association**

1. Definition: The SDT revised the definition of Transient Cyber Asset 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.

Yes:

No:

**Comments:**

Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Transient Cyber Asset definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.

**Response:**

Thank you for your comment.

The SDT included the referenced language in the definitions to specifically address the fact that ESPs and PCAs are not required to be identified at assets containing low impact BES Cyber Systems. No additional guidance is required.

2. Definition: The SDT revised the definition of Removable Media 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.

Yes:

No:

**Comments:**

Request that the guidance be added to the Guidance and Technical Basis (GTB) on the need for the additional language referencing High and Medium Impact with regard to ESP's and PCA's to the Removable Media definition. Guidance would show that low impact BES Cybers Systems may be configured in a way that would meet the definition of ESP even though an ESP is not required or been identified.

**Response:**

Thank you for your comment.

The SDT included the referenced language in the definitions to specifically address the fact that ESPs and PCAs are not required to be identified at assets containing low impact BES Cyber Systems. No additional guidance is required.

3. Requirement R2: The SDT revised CIP-003-7(i), Attachment 1, adding Section 5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation to reflect the mandatory requirement for the Responsible Entity to develop and implement security plans to mitigate the risk of 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.

Yes:

No:

**Comments:**

1) The bulleted list creates requirements that are too prescriptive. Use alternative language for Section 5.1 and 5.2 to remove the bullet points (because they may be used against you in some fashion in the future), and re-write the requirements. The bullet points should go into the GTB section so that there is less chance for a misinterpretation or reinterpretation that would require the implementation of more than one of the bulleted point in order to meet compliance.

2) As written, the requirements listed for TCAs in CIP-003-7(i) for Low Impact assets is a subset of the requirements for high and medium impact included in CIP-010-2 R4. If this list remains the same or if changed the GTB section should include a statement that low impact requirements are a subset of those for High and Medium.

**Response:**

Thank you for your comments.

The use of the bulleted list is consistent with other currently approved standards. The SDT's intention in using the bulleted list is to provide options to satisfy the parent statement, and the SDT purposely included the ability for the Responsible Entity to use other protection methods, rather than those listed, that more adequately fit the entity's environment.

The relationship between highs, mediums, and lows is addressed in Attachment 1 to allow entities to utilize a single program for all impact levels.

4. Attachment 2: The SDT revised the evidential language of CIP-003-7(i), Attachment 2, Section 5 to make the Measures consistent with the requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

Yes:

No:

**Comments:**

The complexity of the sentences are difficult to read and understand. Suggest revising to bulleted lists. The evidence requirements seem to require an inventory of TCA's and Removable Media. This could be a significant burdent on registered entities in the same way that a list of BES Cyber Systems has been determined to be an issue.

**Response:**

Thank you for your comment.

While the SDT thanks you for the comment, we decline to make the suggested modification to the format. Although the definition of TCA references BES Cyber Assets (BCA), a discrete list of BCAs or BES Cyber Systems is not required. However, in accordance with CIP-002-5.1 R1.3, a Responsible Entity must be able to identify assets that contain low impact BES Cyber Systems, and must have a plan (in accordance with Section 5 of Attachment 1, CIP-003-7(i)), to identify any Removable Media prior to connecting it to a low impact BES Cyber System(s).

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.

Yes:

No:

**Comments:**

1) The guidance should be coordinated with the Supply Chain SDT.

2) The GTB language that states: “Section 5.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.” is too prescriptive. Recommend that the “are to” be changed to “may”. The use of prescriptive language like “should” and “are to” should be used on a very limited basis if not removed entirely. Guidance should be shifted to a programmatic approach.

**Response:**

Thank you for your comments.

The Project 2016-02 Modifications to CIP Standards SDT is coordinating with the Supply Chain SDT as necessary.

The SDT updated the G&TB to more closely align with the requirement language. The intent is to reiterate the need to document and implement the plan as specified in the requirement, not to infer other obligations in the G&TB.

6. Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority’s order approving the standard, 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.

Yes:

No:

**Comments:** None

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.

**Comments:**

1) The word “and” should be added at the end of R1.2.5

2) This comment form did not reference the addition of CIP Exceptional Circumstances in Requirement R1.2.6 and the inclusion of the phrase “except under CIP Exceptional Circumstances” in Attachment 1, Section 5. The “except under CIP Exceptional Circumstances” phrase should also be addressed in Attachment 1 Sections 2 and 3. Not addressing CIP Exceptional Circumstances in Sections 2 and 3 may result in a “no” vote on future ballot of this standard.

3) A Section 6 under Attachment 2 is needed to explain how the CIP Exceptional Circumstance is to be used so you can put it into your policy/plan accordingly.

**Response:**

Thank you for your comments.

The word "and" was added to Requirement R1.2.5.

Due to the requirement to perform actions at the time of use of a TCA or RM, an entity may not be able to perform the controls prescribed under Section 5 during a CEC. Therefore, the CEC language was added to address this situation. The other sections under Attachment 1 do not have the same timing aspects as Section 5. The SDT will be seeking industry feedback on the applicability of CEC to other requirements and parts. Requirement 1.2.6 was added to ensure a policy for CEC in the use of TCA and RM. Guidance was added for policy section 1.2.6 on declaring and responding to CEC.

**End of Report**