

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2016-02 CIP Modifications

Webinar on SDT Proposals for Stakeholder Comment/Ballot
October 25, 2016

RELIABILITY | ACCOUNTABILITY



NERC Antitrust Guidelines

- It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

Notice of Open Meeting

- Participants are reminded that this webinar is public. The access number was widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

	Name	Entity
Chair	Margaret Powell	Exelon
Vice Chair	Christine Hasha	Electric Reliability Council of Texas
Vice Chair	David Revill	Georgia Transmission Corporation
Members	Steven Brain	Dominion
	Jay Cribb	Southern Company
	Jennifer Flandermeyer	Kansas City Power and Light
	Tom Foster	PJM Interconnection
	Richard Kinas	Orlando Utilities Commission
	Forrest Krigbaum	Bonneville Power Administration
	Philippe Labrosse	Hydro-Quebec TransEnergie
	Mark Riley	Associated Electric Cooperative, Inc.

- Revisions will cover eight issue areas:
 - LERC definition (Order 822) – deadline of March 31, 2017
 - Transient devices used at low-impact BES Cyber Systems (Order 822)
 - Communication network components between BES Control Centers (Order 822)
 - Cyber Asset and BES Cyber Asset Definitions (V5TAG)
 - Network and Externally Accessible Devices (V5TAG)
 - Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations (V5TAG)
 - Virtualization (V5TAG)
 - CIP Exceptional Circumstances
- Plus, the SDT serves as an IDT to consider one Request for Interpretation concerning shared BES Cyber Systems

- Second proposal posted for stakeholder comment
- Proposal includes:
 - Modifications to CIP-003, R2, Attachment 1, Sections 2 and 3
 - Revision to retire Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP)
 - Implementation date proposal of 12 months from approval
 - Consideration of directives
 - VRF and VSL justification
 - Comment form
 - Response to comments from the prior ballot
- Comment period: October 21 – December 5, 2016
- Ballot period: November 23 – December 5, 2016

- Initial ballot results for LERC posting:
 - Draft CIP-003-7 standard received 41.54% approval
 - Draft LERC definition received 30.63% approval
- SDT reviewed themes from industry comments:
 - Concerns regarding the scope expanding to non-BES Cyber Systems
 - Revisions went beyond the FERC directive to address the term direct in the definition
 - Lack of clarity on the concept of “asset boundary”
 - Support for the reference models in the Guidelines & Technical Basis, including requests for additional reference models
 - Implementation plan concerns on the existing “-6” standard with a “-7” standard in development
 - Support for a single implementation plan date, but requested additional time

- The SDT reviewed three paths forward for the LERC revisions:
 - Option 1: Revert back to original language and clarify the word “direct”
 - Option 2: Stay the course with the draft language, but add an exclusion for those connections that have nothing to do with the BES
 - Option 3: Eliminate the term “LERC” by incorporating the LERC concepts into the requirement language (similar to CIP-003, Attachment 1, Section 2 Physical Security Controls)

- The team reached consensus to focus on “option 3” to remove LERC:
 - Focuses on “access” to low impact BES Cyber Systems rather than the BES asset
 - Emphasizes achieving the security objective of implementing security controls rather than making lists (documenting) where LERC exists
 - Because the term LERC is used in only one standard (CIP-003), more clarity is provided by incorporating the language of the LERC definition into the standard (Attachment 1, Section 3.1 and eliminating the defined term)

- CIP-003-7, Attachment 1, Section 2:

Section 2. Physical Security Controls: *Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.*

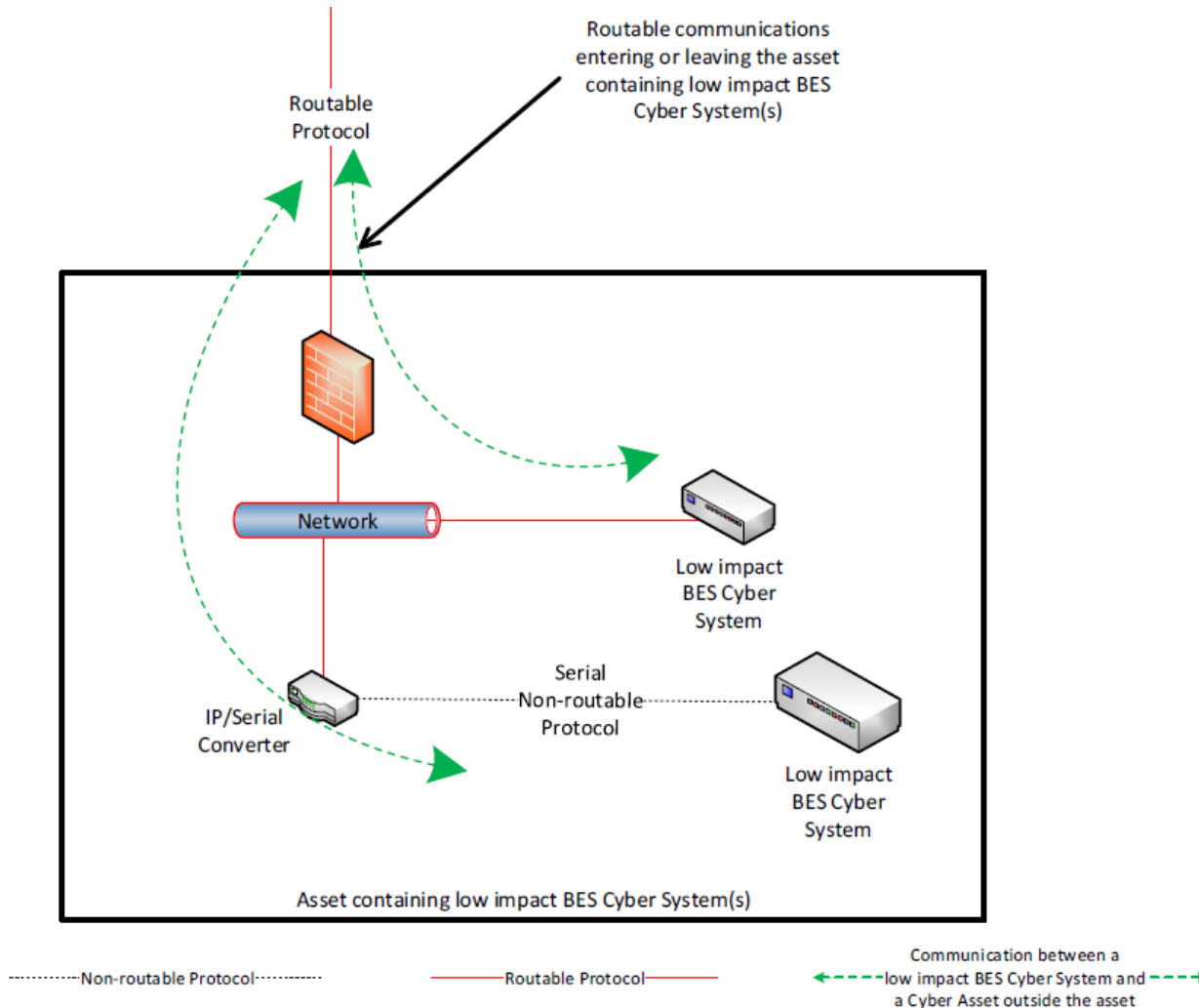
- CIP-003-7, Attachment 1, Section 3:

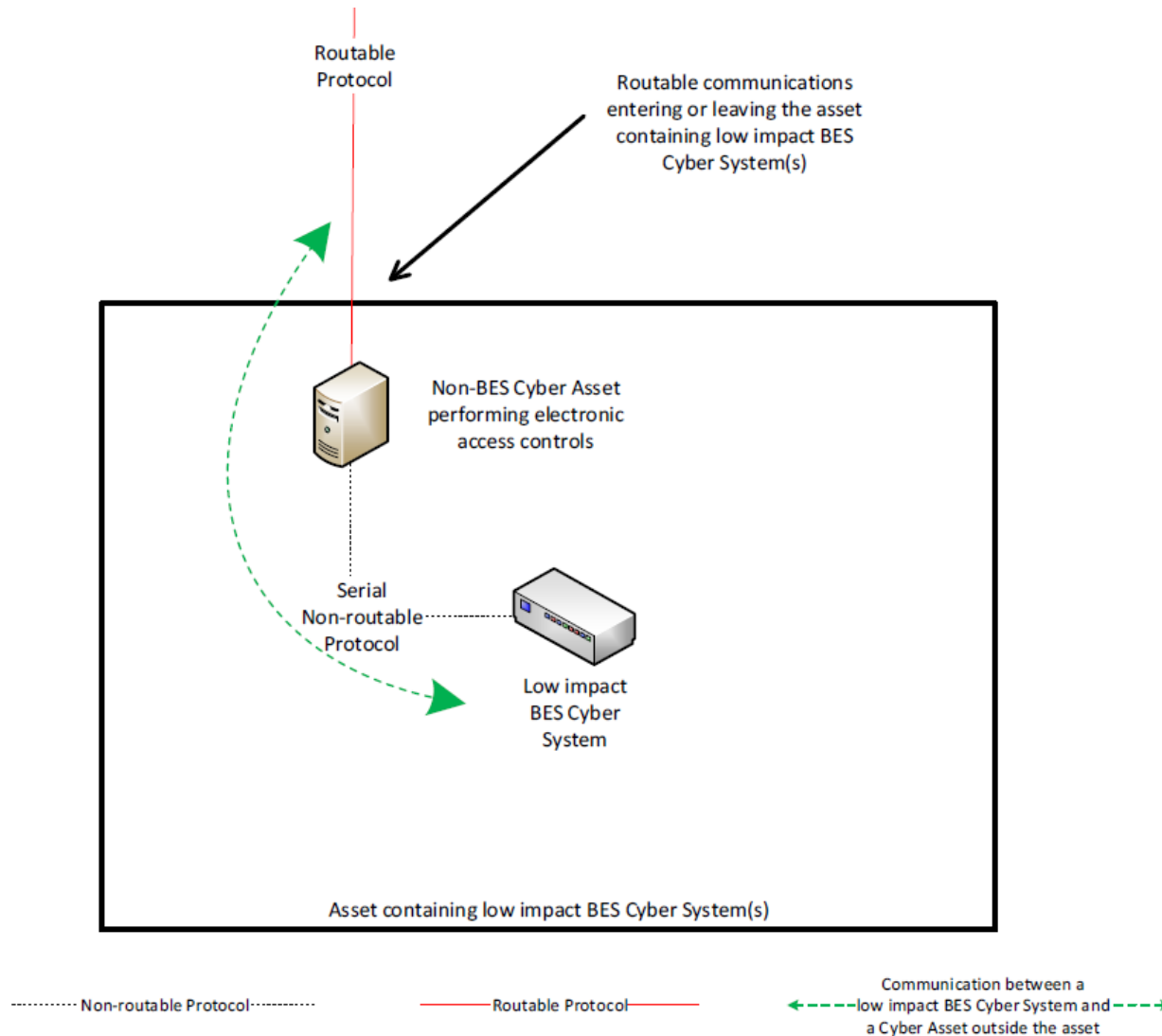
Section 3. Electronic Access Controls: *For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:*

3.1 *Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:*

- i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);*
- ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and,*
- iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE).*

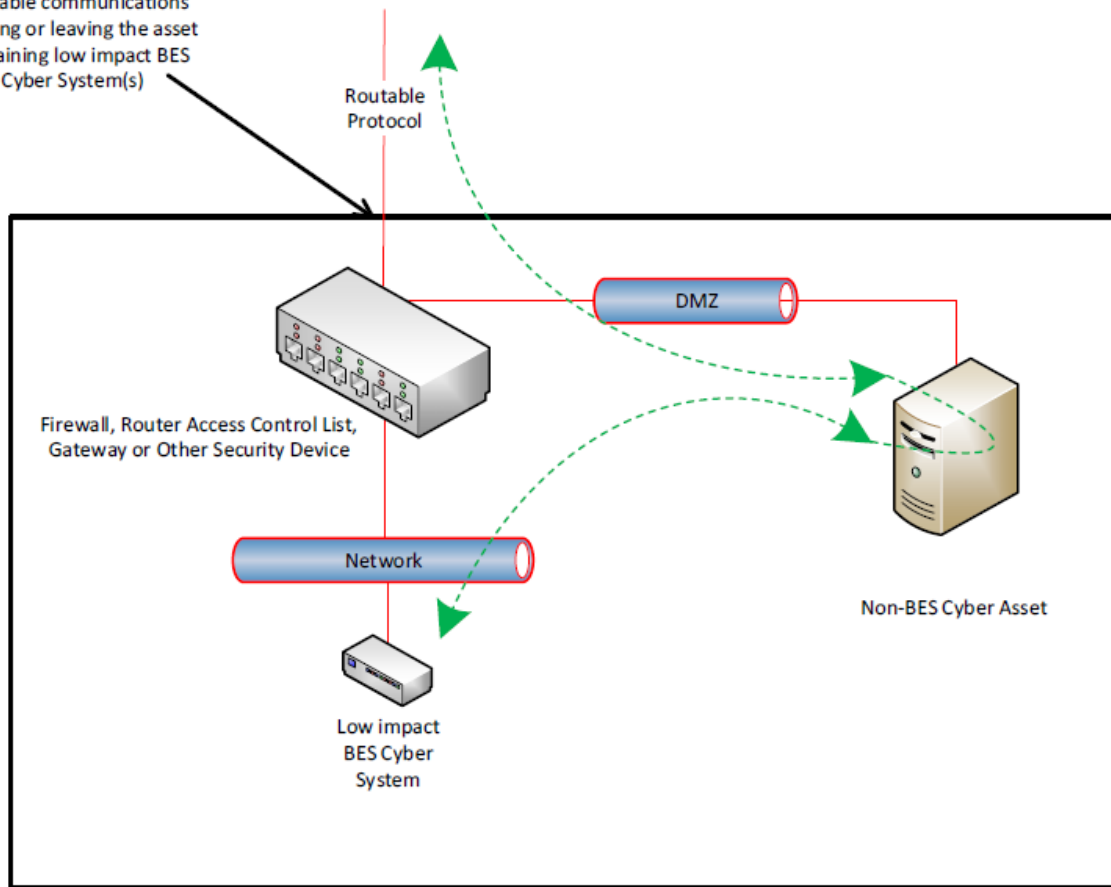
3.2 *Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.*





Reference Model 6 – Indirect Access

Routable communications entering or leaving the asset containing low impact BES Cyber System(s)

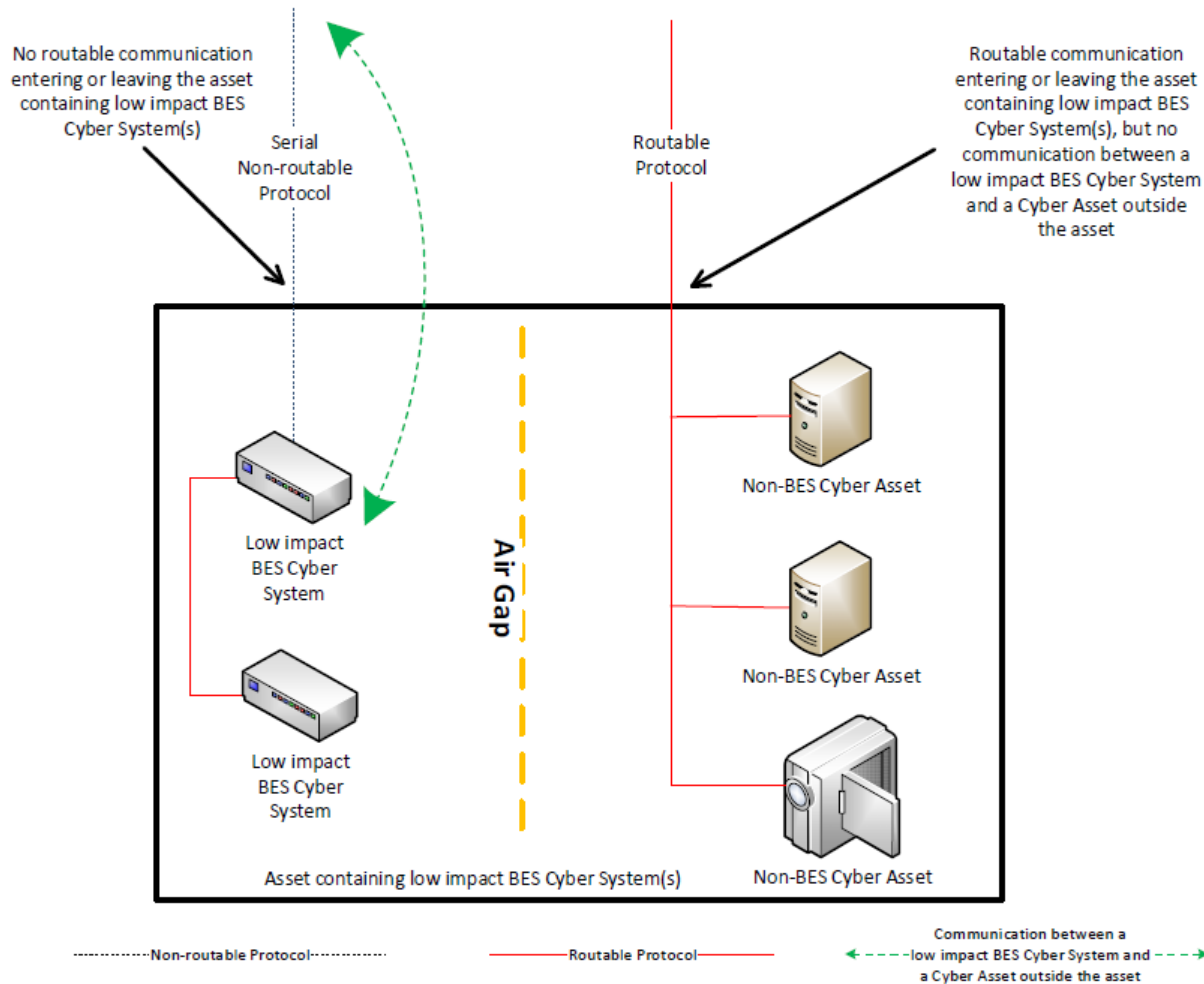


..... Non-routable Protocol

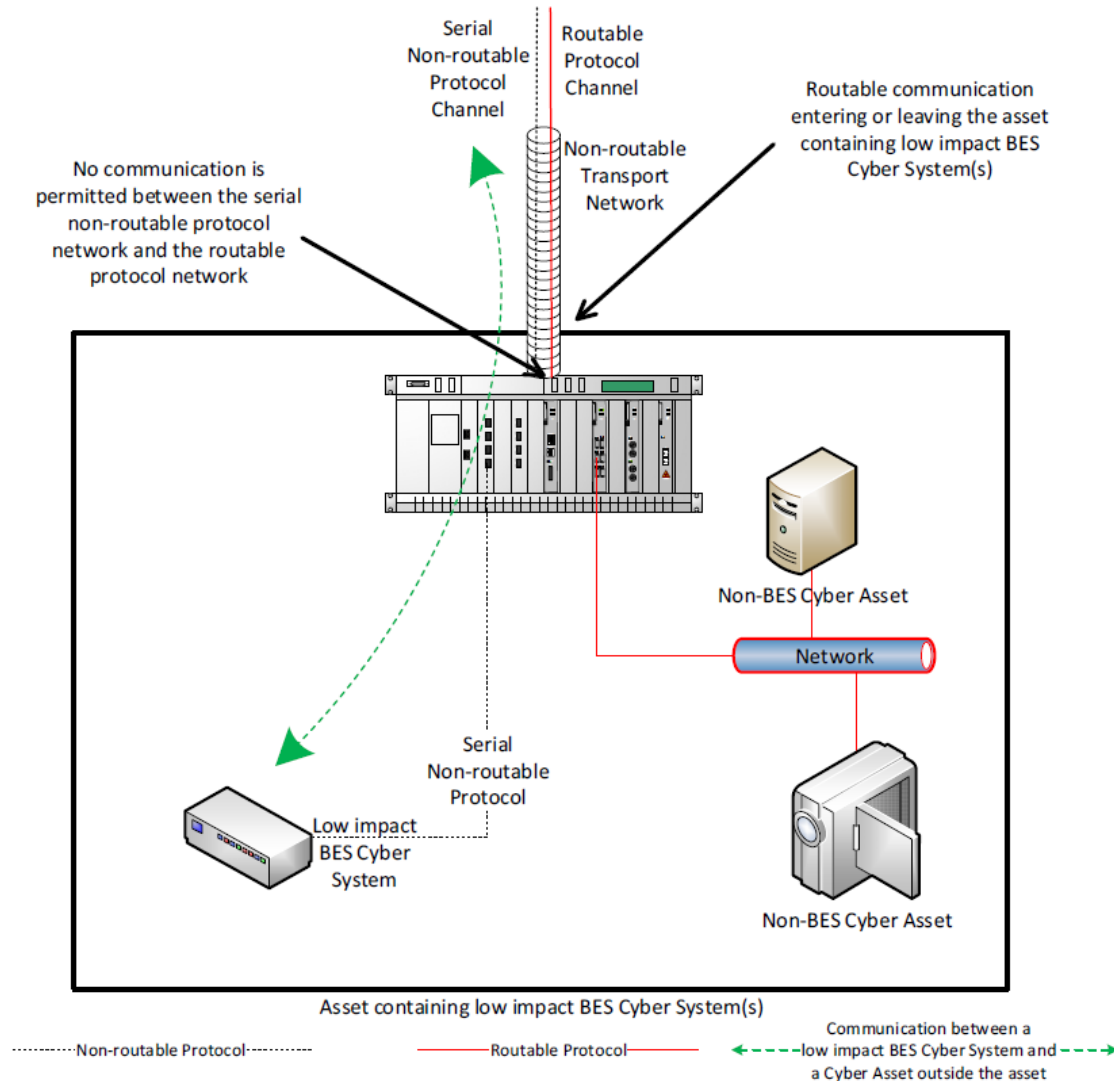
———— Routable Protocol ————

← - - - - Communication between a low impact BES Cyber System and a Cyber Asset outside the asset - - - - →

Reference Model 8 – Physical Isolation and Serial Non-routable Communications



Reference Model 10 – Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network



The effective date for the proposed Reliability Standard is provided below:

- Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-7 shall become effective on the later of September 1, 2018 or the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.
- Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-7 shall become effective on the first day of the first calendar quarter that is twelve (12) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

General Considerations:

- Requirement 2, Attachment 1, Sections 1 and 4 will be effective with CIP-003-6
- Requirement 2, Attachment 1, Sections 2 and 3 shall be replaced with the effective date of CIP-003-7.

- Proposal package to be submitted to the Standards Committee to authorize posting
- Proposal includes:
 - Revised Definition to accommodate use at all impact levels - Highs, Mediums, and Lows
 - Addition of TCAs to CIP-003, R2, Attachment 1, Section 5
 - Language consistent with CIP-010 to accommodate programs already in development and implementation, and enable extension of CIP-010 to incorporate lows
 - Corresponding Measures, Guidelines and Technical Basis, and VSLs
 - Implementation date proposal of 12 months from approval

Revised “Transient Cyber Asset” (TCA) Definition

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

Examples of TCAs include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes

Section 5. *Transient Cyber Asset and Removable Media Malicious Code Mitigation Plan(s): Each Responsible Entity shall implement one or more plan(s) to achieve the objective of mitigating the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media, which shall include:*

5.1 *For Transient Cyber Asset(s) managed by the Responsible Entity, if any, use of one or a combination of the following methods 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.*

5.2 *For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any, use of one or a combination of the following methods prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):*

- *Review of antivirus update level;*
- *Review of antivirus update process used by the party;*
- *Review of application whitelisting used by the party;*
- *Review use of live operating system and software executable only from read-only media;*
- *Review of system hardening used by the party; or*
- *Other method(s) to mitigate the introduction of malicious code.*

5.3 *For Removable Media, perform each of the following:*

5.3.1 *Use of 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.*

The effective date for the proposed Reliability Standard is provided below:

- Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-7(i) and the NERC Glossary term Transient Cyber Asset (TCA) shall become effective on the later of September 1, 2018 or the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard and NERC Glossary term, or as otherwise provided for by the applicable governmental authority.
- Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-7(i) and the NERC Glossary term Transient Cyber Asset (TCA) shall become effective on the first day of the first calendar quarter that is twelve (12) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Standard/Requirement	NERC Board Adoption	Order 822 Effective Date: March 31, 2016	VS Enforcement Date***	If effective date of the FERC approval, then LERC revisions become effective:					
		Compliance Deadline		2Q17	3Q17	4Q17	1Q18		
CIP-002-5	IAC, CN revisions - November 13, 2014 LI, TD revisions - February 12, 2015	1-Jul-16	July 1, 2016 - CIP V5 Approved Compliance Date						
CIP-003-6		1-Jul-16		1-Jul-16	1-Jul-16	1-Jul-16	1-Jul-16		
CIP-003-6, R1, part 1.1*		1-Jul-16		1-Jul-16	1-Jul-16	1-Jul-16	1-Jul-16		
CIP-003-6, R1, part 1.2		1-Apr-17		1-Apr-17	1-Apr-17	1-Apr-17	1-Apr-17		
CIP-003-6, R2		1-Apr-17		1-Apr-17	1-Apr-17	1-Apr-17	1-Apr-17		
CIP-003-6, Att 1, Sect. 1		1-Apr-17		1-Apr-17	1-Apr-17	1-Apr-17	1-Apr-17		
CIP-003-7, Att 1, Sect. 2		1-Sep-18		1-Sep-18	1-Jan-19	1-Apr-19	1-Apr-19		
CIP-003-7, Att 1, Sect. 3		1-Sep-18		1-Sep-18	1-Jan-19	1-Apr-19	1-Apr-19		
CIP-003-6, Att 1, Sect. 4		1-Apr-17		1-Apr-17	1-Apr-17	1-Apr-17	1-Apr-17		
CIP-004-6		1-Jul-16							
CIP-005-5		1-Jul-16							
CIP-006-6		1-Jul-16							
CIP-006-6, R1, part 1.10**		1-Apr-17							
CIP-007-6		1-Jul-16							
CIP-007-6, R1, part 1.2**		1-Apr-17							
CIP-008-5		1-Jul-16							
CIP-009-6		1-Jul-16							
CIP-010-2		1-Jul-16							
CIP-010-2, R4		1-Apr-17							
CIP-011-2		1-Jul-16							
TCA, RM Glossary Terms		1-Apr-17							
BCA, PCA Glossary Terms		1-Apr-17							
LERC, LEAP Glossary Terms		1-Apr-17							
All dates and deadlines remain active under CIP V6 implementation plan									
				Retirement of Terms					

- The initial ballot on the EnergySec Interpretation of CIP-002-5.1 received 91.68% approval receiving 16 negative votes with comment
- IDT reviewed and responded to all comments
- Final ballot October 13-24, 2016

- This slide deck and other information relative to the CIP Modifications SDT can be found on the Project 2016-02 Project Page under Related Files:

[Project 2016-02 Modifications to CIP Standards](#)

- The Interpretation of CIP-002-5.1 for Energy Sector Security Consortium (EnergySec) may be found on the Project 2015-INT-01 Project Page:

[Project-2015-INT-01 Interpretation of CIP-002-5-1 for EnergySec](#)



Questions and Answers