NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Project 2016-02
# CIP Modifications

Webinar on Revisions in Response to LERC Directive

August 16, 2016

RELIABILITY | ACCOUNTABILITY

# Administrative Items

- 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.

# The CIP Standard Drafting Team

| | 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. |
| | Zach Trublood | Sacramento Municipal Utility District |

# Webinar Agenda

- Introductions
- Opening Remarks
- Approach to the Revisions
- LERC Definition Update and Retirement of LEAP
- CIP-003-7, Attachment 1 - Requirements
- CIP-003-7, Attachment 2 - Measures
- Guidelines and Technical Basis, Reference Models
- Implementation Plan
- Next Steps

# Approach to Clarify LERC Definition

- The SDT considered two approaches to address the directive to clarify ‘direct’.
  - Option 1 – Revise the LERC definition to enable a security control external to the BES Cyber Asset (such as an application break) to indicate the absence of LERC
  - Option 2 – Revise the LERC definition to identify all routable protocol communications crossing the asset boundary without regard to 'direct vs. indirect' access. Also, revise the CIP-003 requirements to implement electronic access controls and update and expand the Guidelines and Technical Basis.
- Both options meet the same security objective.
- The SDT selected Option 2 - to revise the definition, requirement language, and guidelines and technical basis.

# LERC Definition

- Changed Low Impact External Routable Connectivity to Low Impact External Routable Communication (LERC) to focus on the communication that occurs crossing the boundary of the asset containing the low impact BES Cyber Systems to more cleanly align with the output of CIP-002-5.1 R1, Part 1.3.
- Removed from the definition the word ‘direct’ thus expanding the LERC definition to be inclusive of both direct and indirect connections.
- Simplified LERC as an attribute of a BES asset concerning whether there is routable protocol communications across the asset boundary.
- Removed the dependency between the electronic access controls that may be in place and having those controls determine whether LERC exists or not.

# LERC Definition

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

- **Current Definition: Low Impact External Routable Connectivity (LERC):** Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

# Retirement of LEAP

- The changes to LERC changed the focus of the CIP-003 requirements and no longer emphasized the “interface” that controlled the connectivity.
  - **Current Term: Low Impact BES Cyber System Electronic Access Point” (LEAP):** A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems.
- As a result, the SDT removed use of the term “LEAP” and proposed its retirement.

# CIP-003-7 Requirements

- For those BES assets that have LERC, the SDT changed the requirement to requiring electronic access controls to "permit only necessary electronic access to low impact BES Cyber Systems."
- The SDT also revised CIP-003-6, Attachment 1, Section 2 to accommodate the retirement of LEAP in the physical security section and to provide for the physical security of the Cyber Assets performing the electronic access controls required in Section 3.

# CIP-003-7 Requirements (Attachment 1)

**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 Low Impact BES Cyber System Electronic Access Points (LEAPs),~~ the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

**Section 3.** Electronic Access Controls: Each Responsible Entity shall:

**3.1** Implement electronic access control(s) for LERC, if any, ~~implement a LEAP~~ to permit only necessary ~~inbound and outbound bi-directional routable protocol access; and~~ electronic access to low impact BES Cyber System(s).

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

# CIP-003 Measures (Attachment 2)

- The SDT revised CIP-003-6, Attachment 2, Sections 2 and 3 to make the Measures consistent with the revised requirement language.

**Section 2.** Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset specified by the Responsible Entity that provides electronic access controls implemented for Section 3.1, if any~~, containing a LEAP~~.

# CIP-003 Measures

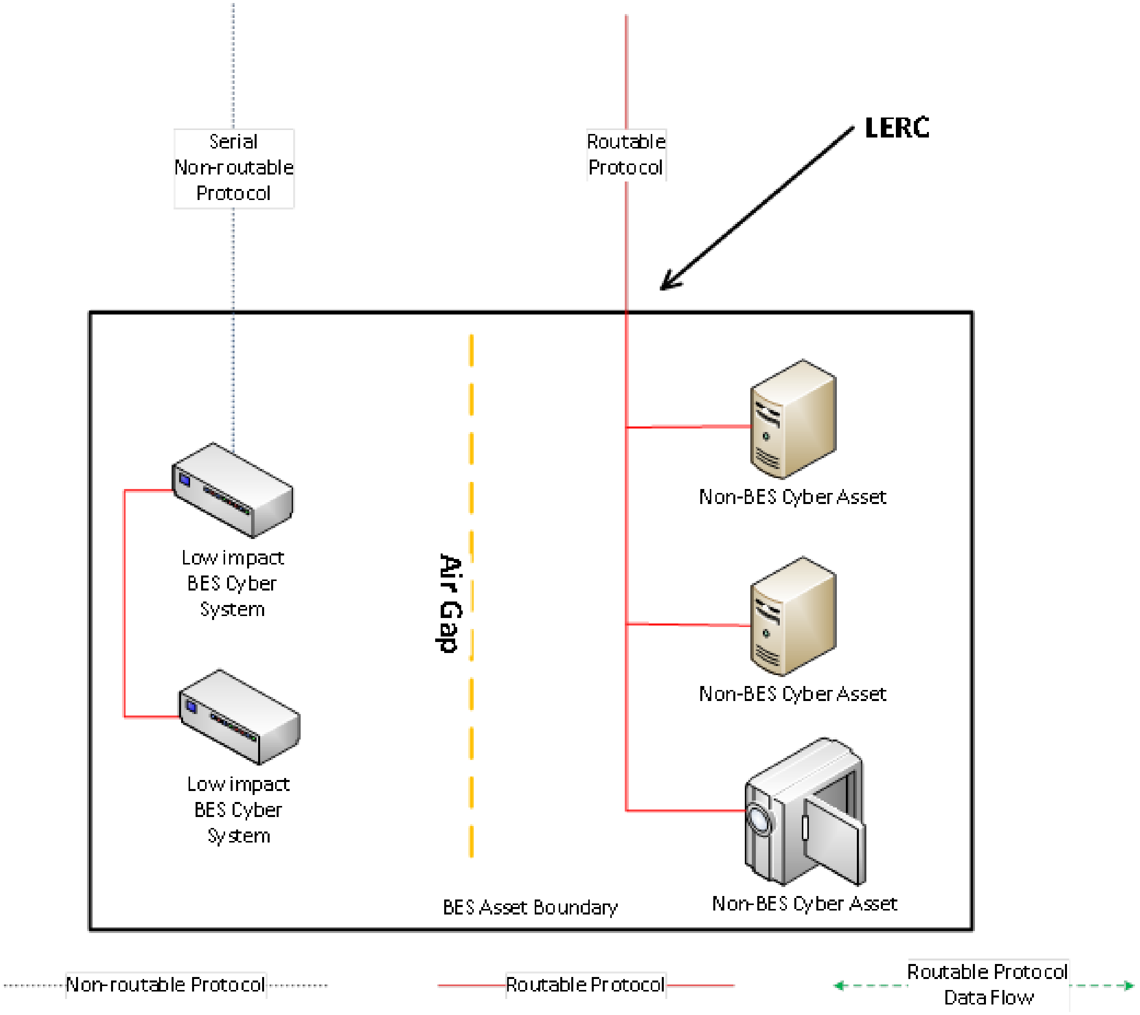
- **Section 3**. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation, such as representative diagrams or lists of implemented electronic access controls (e.g., restricting IP addresses, ports, or services; authenticating users; air-gapping networks; terminating routable protocol sessions on a non-BES Cyber Asset; implementing unidirectional gateways) showing that ~~inbound and outbound connections~~ for ~~any LEAP(s) are~~ LERC at each asset or group of assets containing low impact BES Cyber Systems, is confined ~~to~~ only ~~those~~ to that access the Responsible Entity deems necessary ~~(e.g., by restricting IP addresses, ports, or services)~~; and
2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

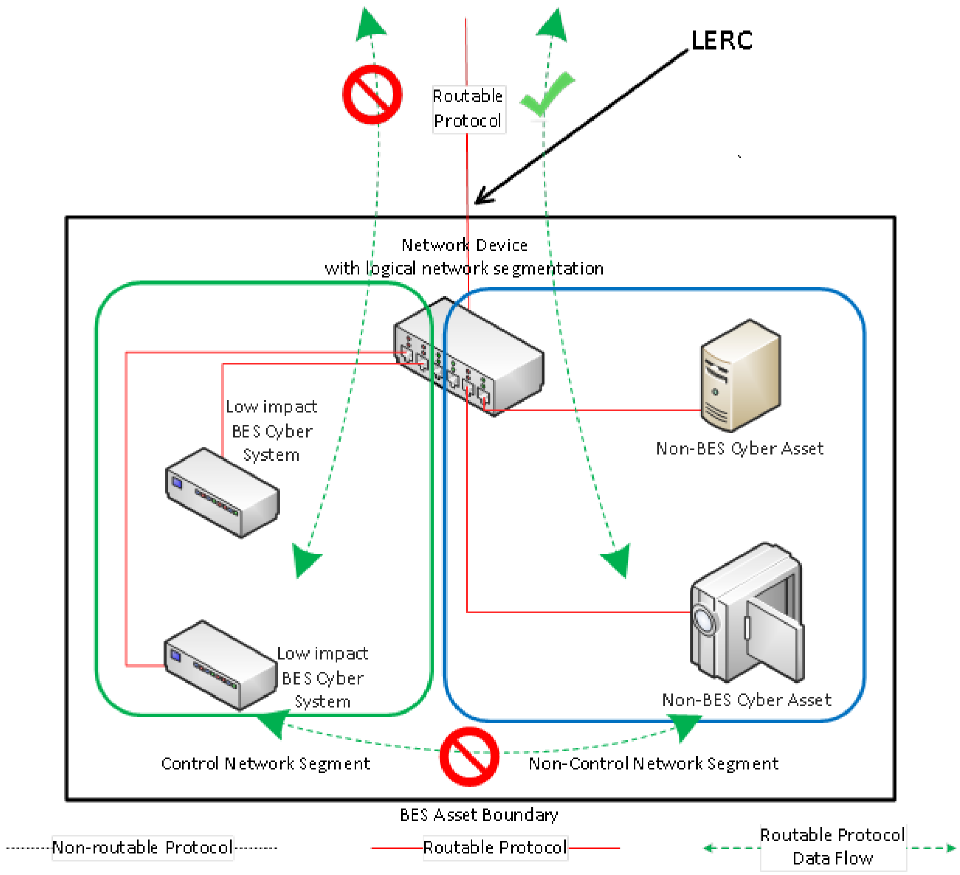
# Asset Boundaries

- Removes ambiguity of *where* routable protocol must exist in current definition (“via a bi-directional routable protocol connection”)
- Used for determining which routable protocol communications and networks are *internal* or *inside* or *local* to the BES asset and which are *external* to or *outside* the BES asset.
- Not an Electronic Security Perimeter or Physical Security Perimeter

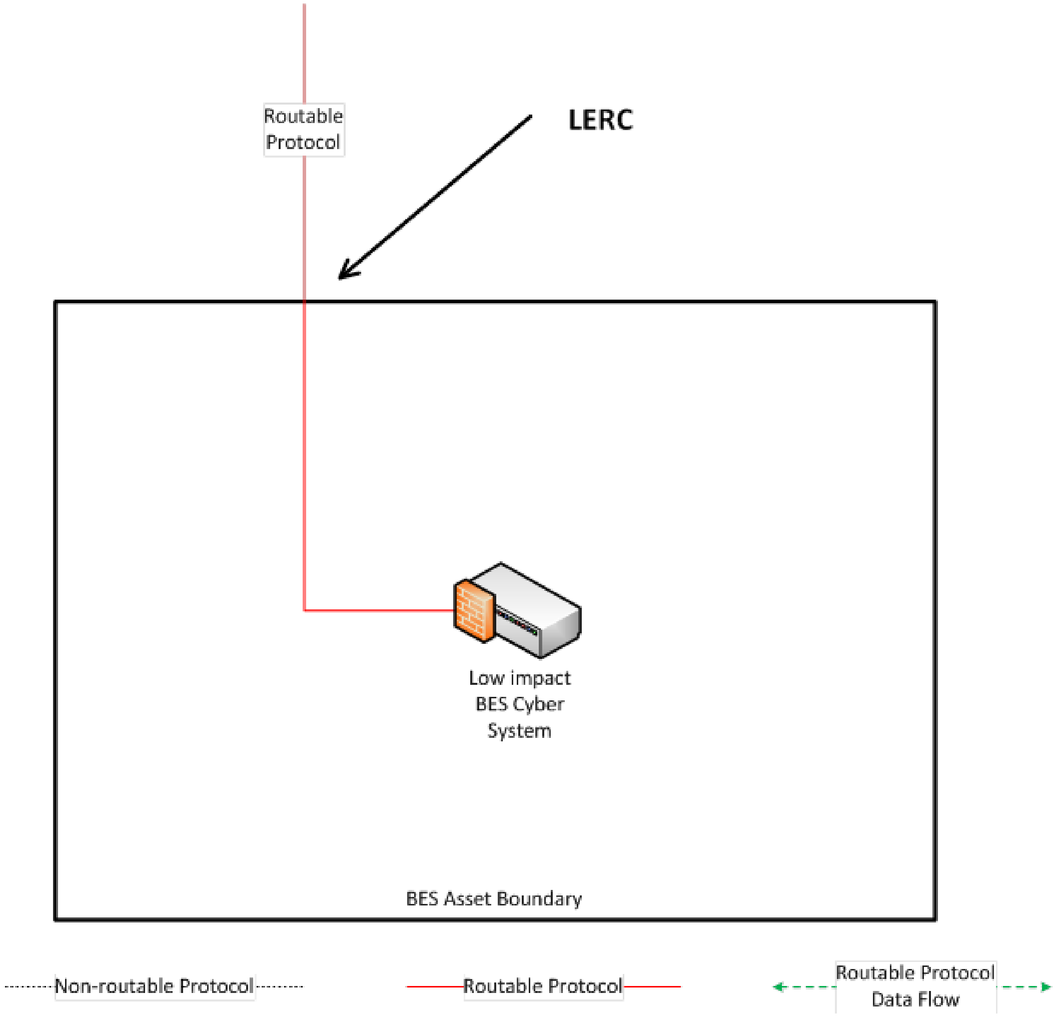
# LERC Reference Model 1



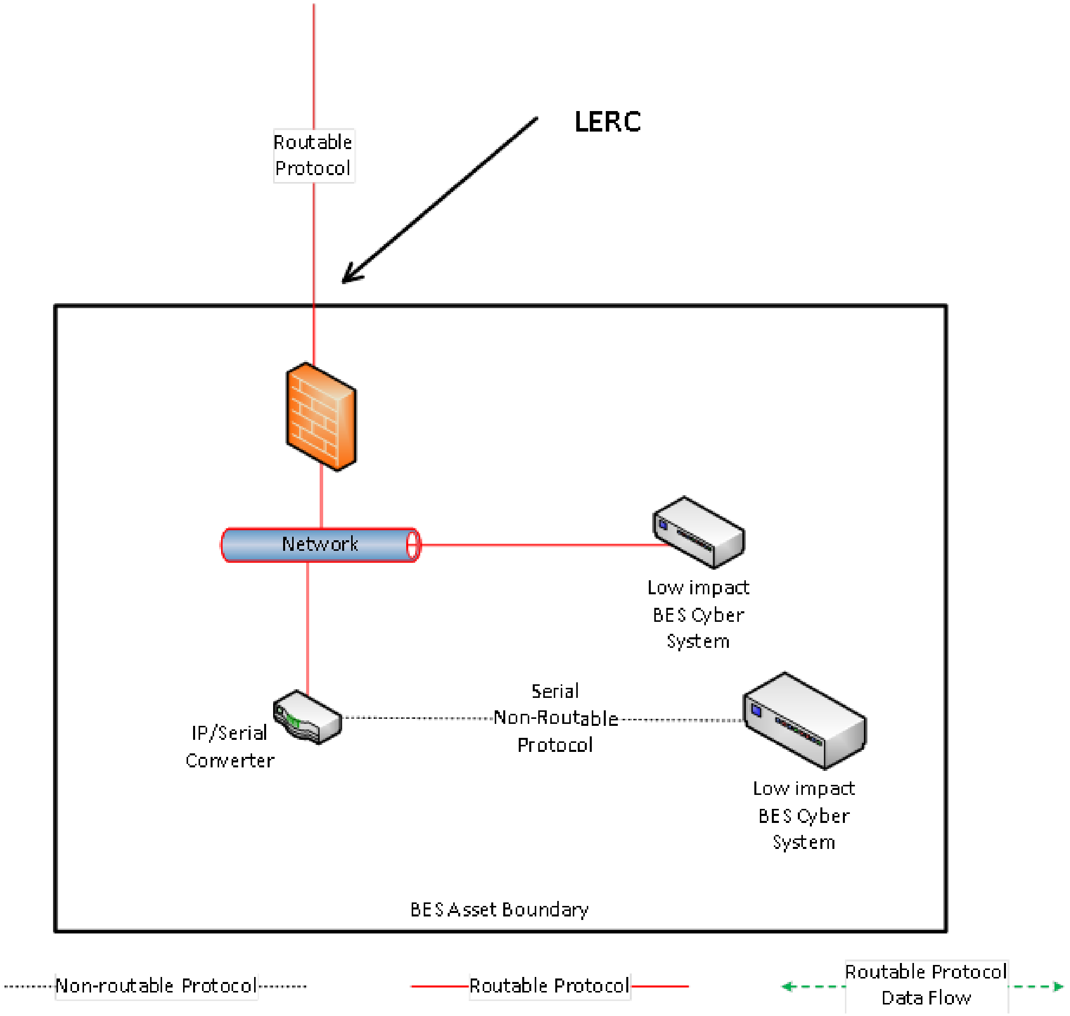
# LERC Reference Model 2



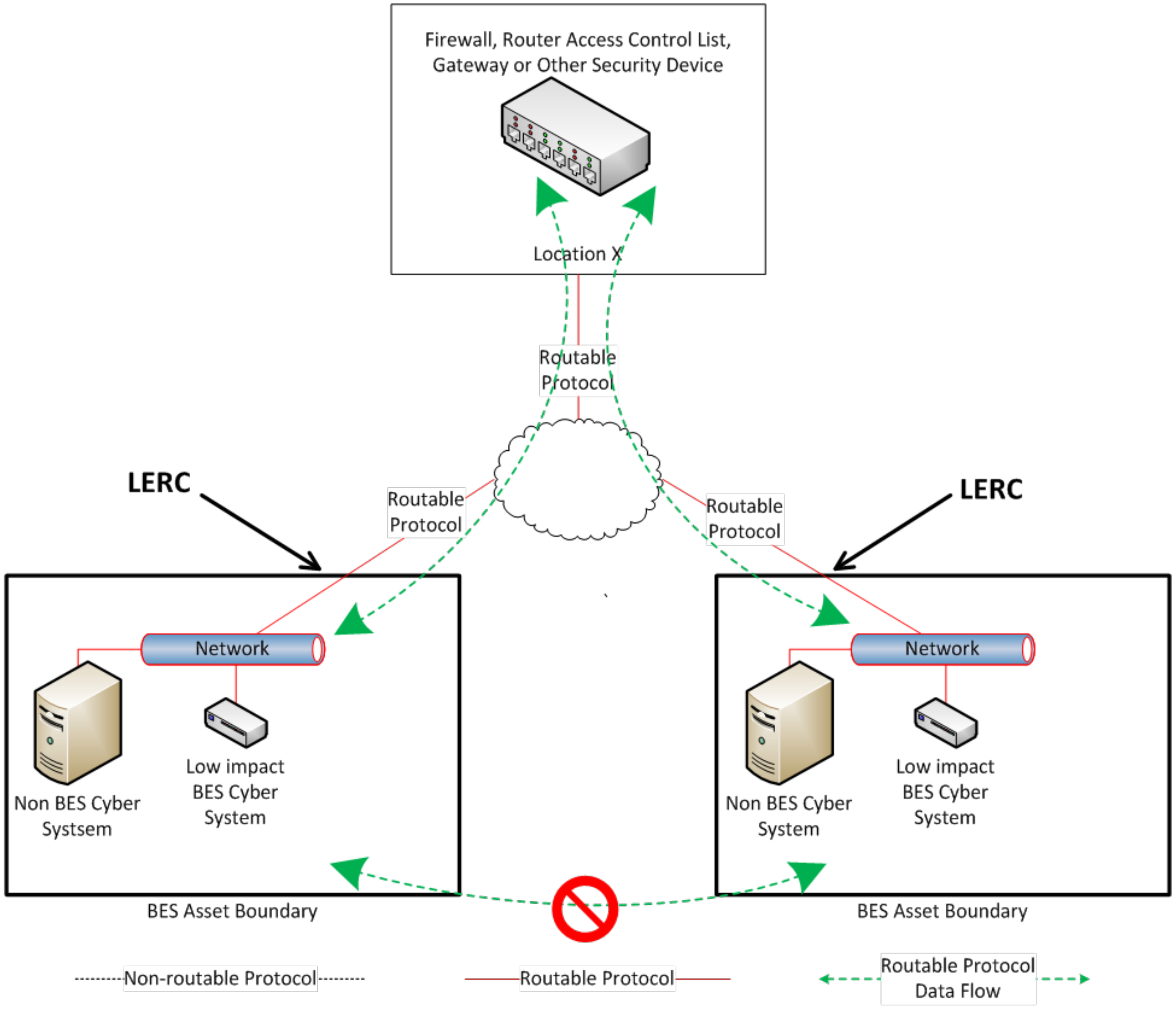
# LERC Reference Model 3



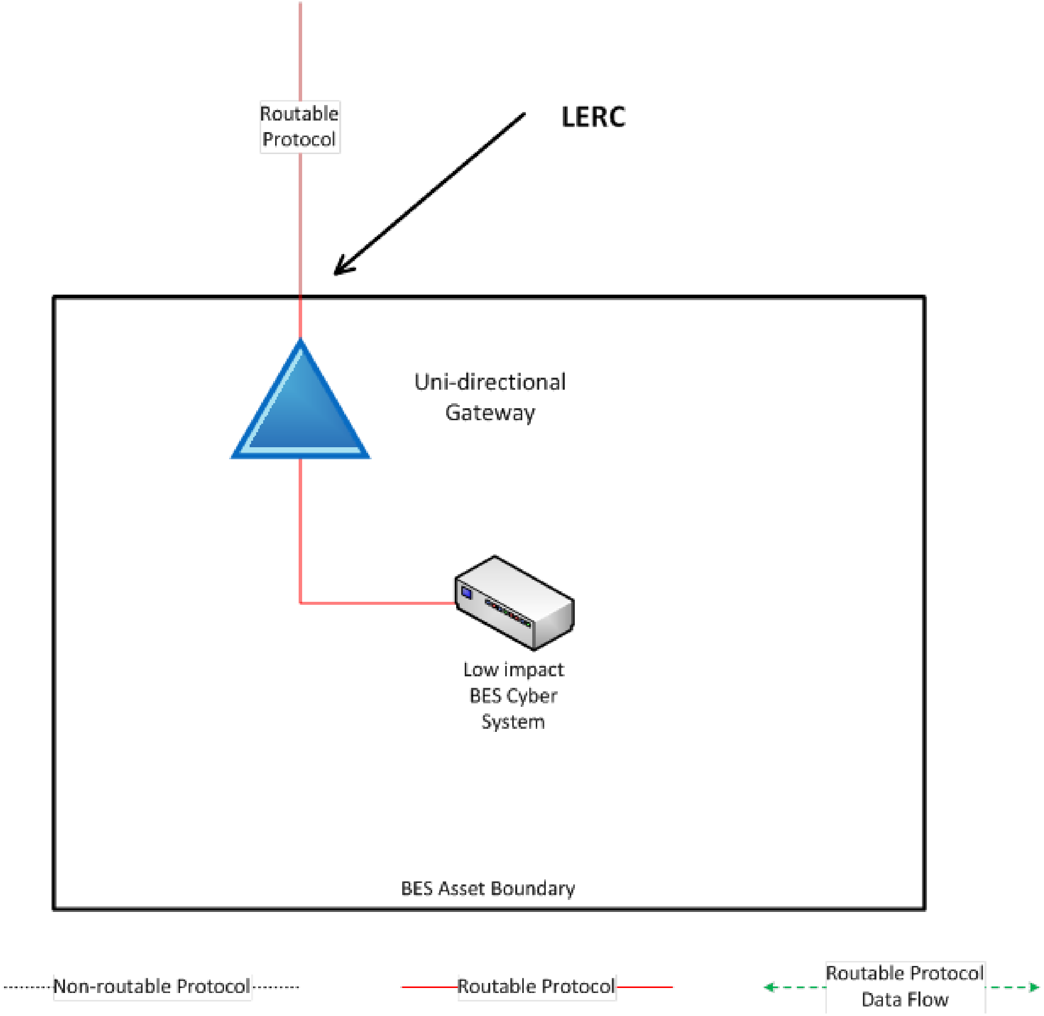
# LERC Reference Model 4


LERC
Routable Protocol
Network
Low impact BES Cyber System
IP/Serial Converter
Serial Non-Routable Protocol
Low impact BES Cyber System
BES Asset Boundary
Non-routable Protocol
Routable Protocol
Routable Protocol Data Flow

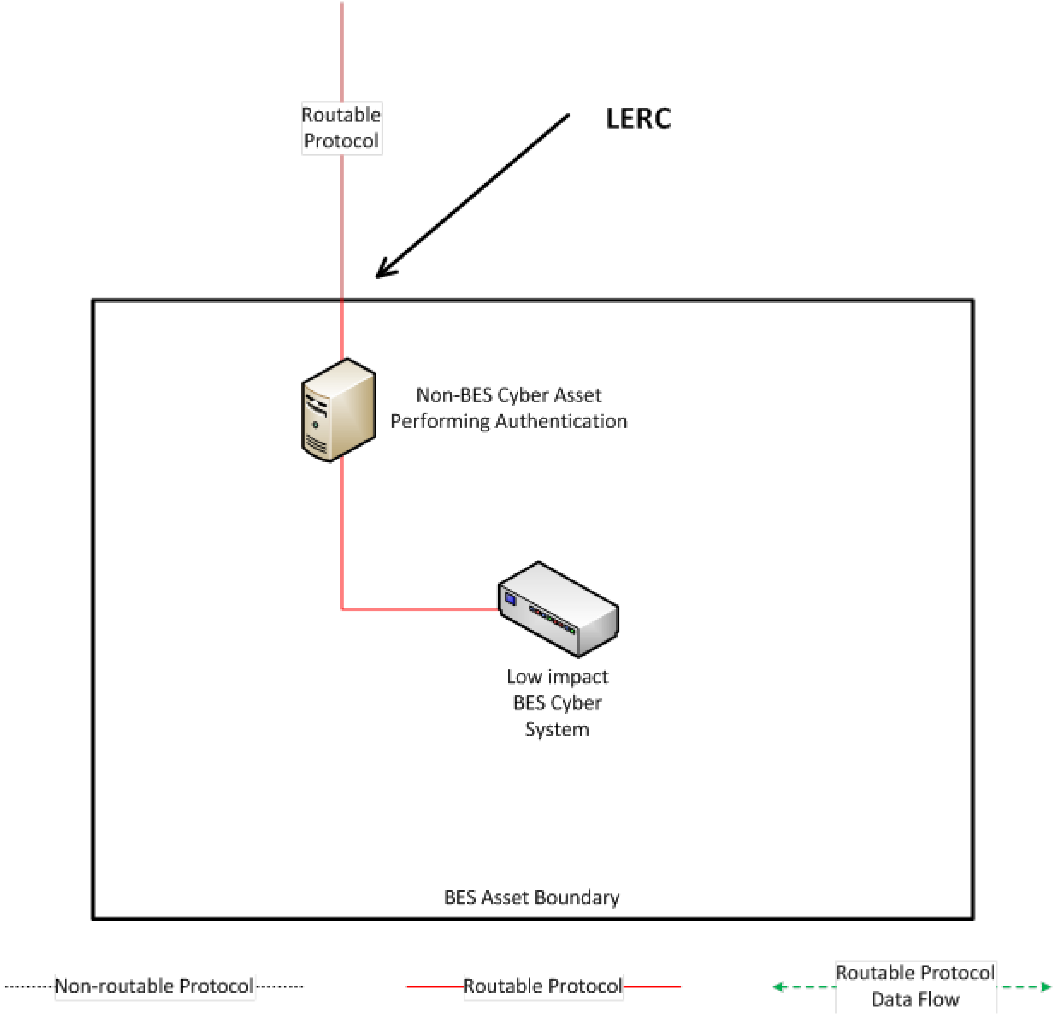
# LERC Reference Model 5



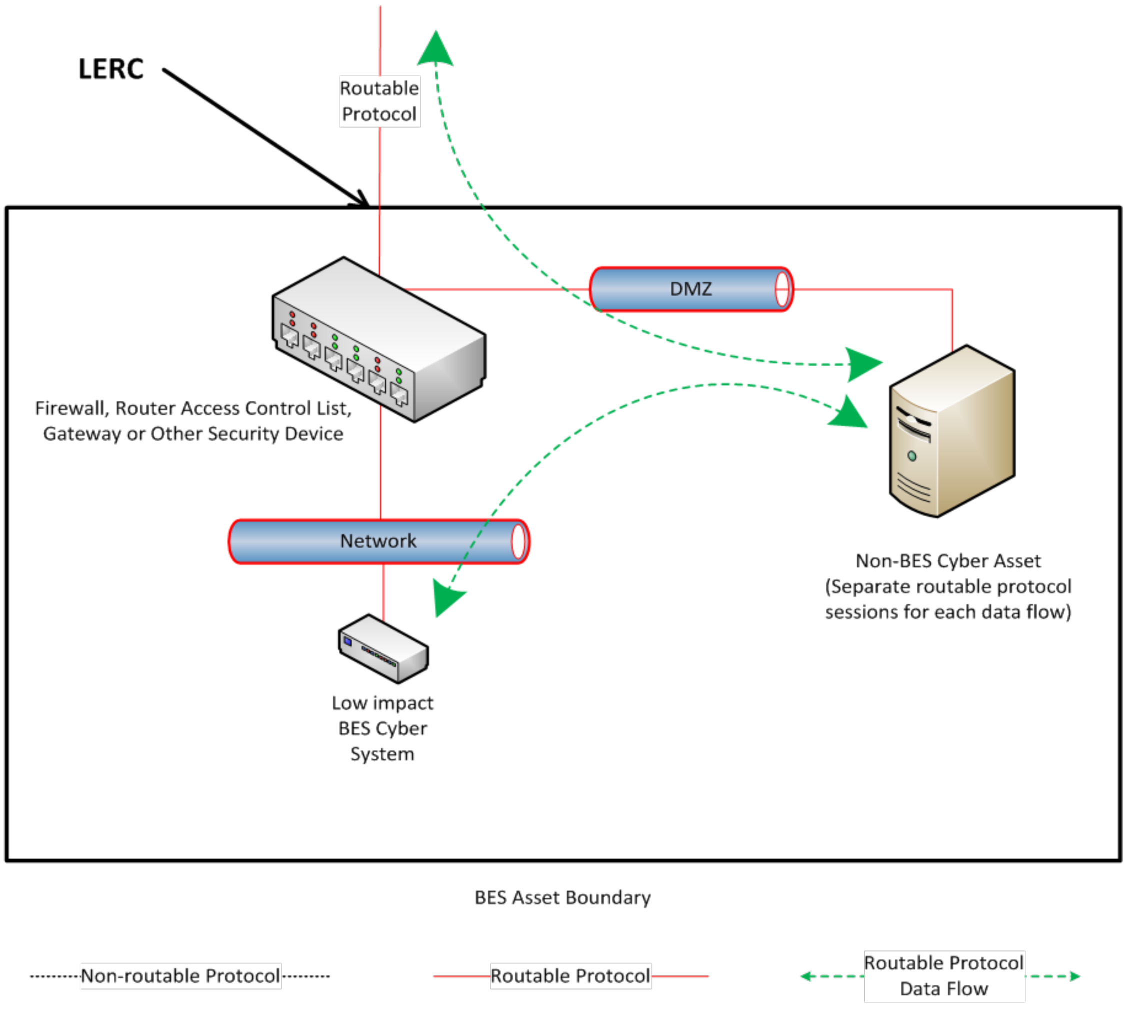
# LERC Reference Model 6



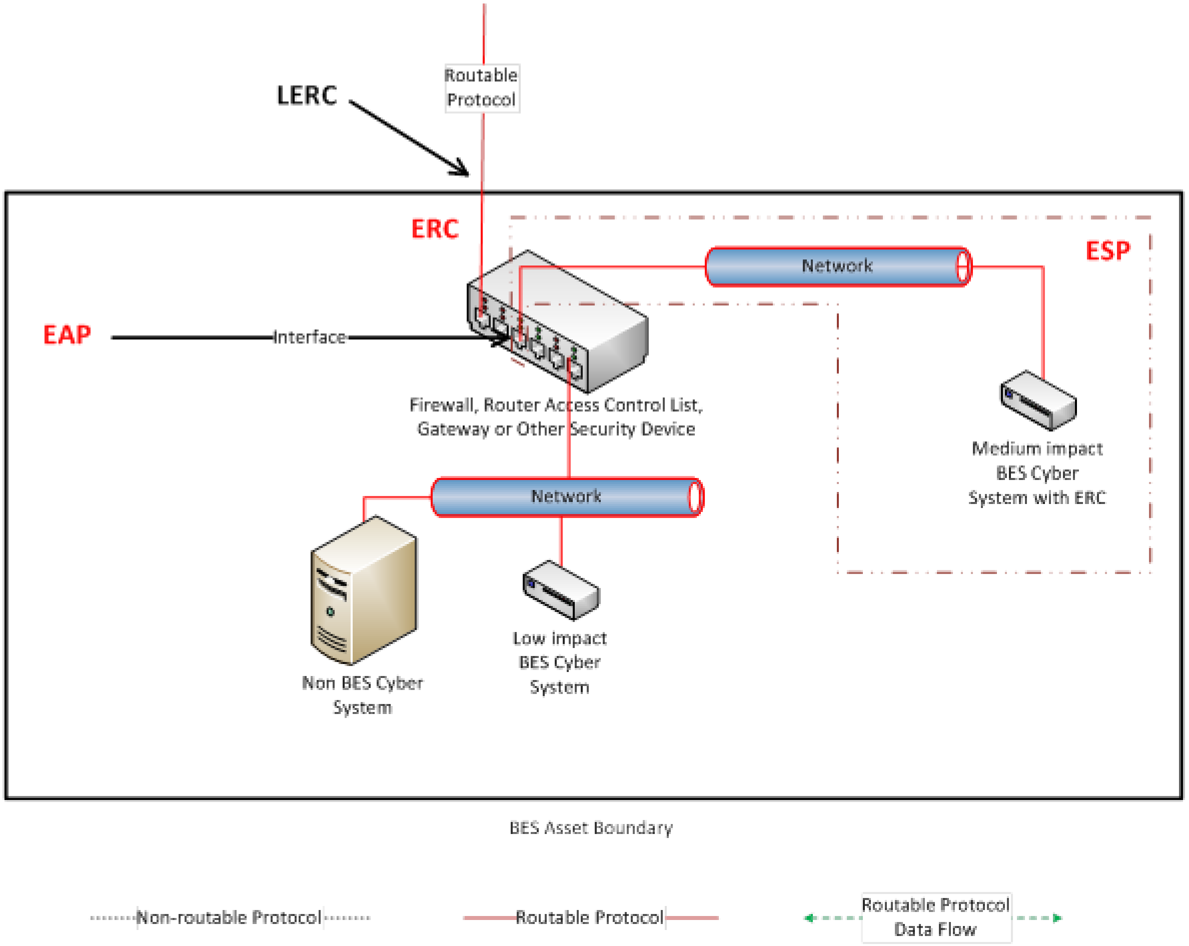
# LERC Reference Model 7


Routable Protocol
LERC
Non-BES Cyber Asset Performing Authentication
Low impact BES Cyber System
BES Asset Boundary
Non-routable Protocol
Routable Protocol
Routable Protocol Data Flow

# LERC Reference Model 8


LERC
Routable Protocol
DMZ
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Non-BES Cyber Asset (Separate routable protocol sessions for each data flow)
Low impact BES Cyber System
BES Asset Boundary
Non-routable Protocol
Routable Protocol
Routable Protocol Data Flow

# LERC Reference Model 9


Routable Protocol
LERC
ERC
ESP
EAP
Interface
Network
Firewall, Router Access Control List, Gateway or Other Security Device
Medium impact BES Cyber System with ERC
Network
Non BES Cyber System
Low impact BES Cyber System
BES Asset Boundary
Non-routable Protocol
Routable Protocol
Routable Protocol Data Flow

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Implementation Plan

- The Implementation Plan does not modify the effective date for CIP-003-6 or any of the phased-in compliance dates in the CIP-003-6 Implementation Plan.
- Provides a single compliance date for the newly revised sections (Sections 2 and 3) in CIP-003-7,  Attachment 1.
- The enforcement deadline will be the later of September 1, 2018 or the first day of the first calendar quarter that is nine (9) calendar months after the effective date of the order providing applicable regulatory approval.
- Carries forward by reference the provisions for planned or unplanned changes.

# Implementation Plan

| | NERC Board Adoption | Order 822 Effective Date: March 31, 2016 | V5 Enforcement Date*** | *If effective date of the FERC approval, then LERC revisions become effective:* | | |
|---|---|---|---|---|---|---|
| Standard/Requirement | | *Compliance Deadline* | | 3Q17 | 4Q17 | 1Q18 |
| CIP-002-5 | IAC, CN revisions - November 13, 2014<br>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 |
| CIP-003-6, R1, part 1.1* | | 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 |
| CIP-003-6, R2 | | 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 |
| **CIP-003-7, Att 1, Sect. 2** | | **1-Sep-18** | | **1-Sep-18** | **1-Oct-18** | **1-Jan-19** |
| **CIP-003-7, Att 1, Sect. 3** | | **1-Sep-18** | | **1-Sep-18** | **1-Oct-18** | **1-Jan-19** |
| CIP-003-6, Att 1, Sect. 4 | | 1-Apr-17 | | 1-Apr-17 | 1-Apr-17 | 1-Apr-17 |
| CIP-004-6 | | 1-Jul-16 | | All dates and deadlines remain active under CIP V6 implementation plan | | |
| 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 | | | | |

# Implementation Plan – Effective Date

*“Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-7 and the NERC Glossary term Low Impact External Routable Communication (LERC) shall become* ***effective on the later of September 1, 2018 or the first day of the first calendar quarter that is nine (9) calendar months after the effective date*** *of the applicable governmental authority’s order approving the standard and NERC Glossary term, or as otherwise provided for by the applicable governmental authority.*

*Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-7 and the NERC Glossary term Low Impact External Routable Communication (LERC) shall become* ***effective on the first day of the first calendar quarter that is nine (9) calendar months after the date the standard is adopted by the NERC Board of Trustees****, or as otherwise provided for in that jurisdiction.”*

# Posting Schedule

LERC

- July 21 - August 19 – Join the Ballot Pools
- July 21 - September 6 – Planned 45 day Comment Period
- August 10 - September 6 – RSAW Comment Period
- August 26 - September 6 – Ballot Period

REMINDER:

CIP-002-5.1 Interpretation

- July 27 - August 25 – Join Ballot Pool
- July 27 - September 12 – Planned 45 day Comment Period
- August 30 - September 12 – Ballot Period

# Resources

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

  http://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx

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

  http://www.nerc.com/pa/Stand/Pages/Project-2015-INT-01-Interpretation-of-CIP-002-5-1-for-EnergySec.aspx

# Questions and Answers