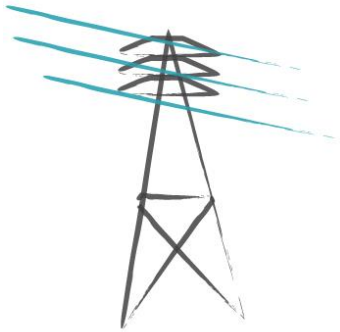


WECC

CIP-012 Developments and Direction

Morgan King CISSP-ISSAP, CISA

Senior Compliance Auditor, Cyber Security

WECC Compliance Workshop – Portland OR – November 14, 2017

Impact to Reliability

Ensure entities are aware of new CIP Compliance Requirements and identify WECC's potential audit approach.

Agenda

- CIP-012-1 Draft 2
- Technical Rationale
- Implementation Guidance

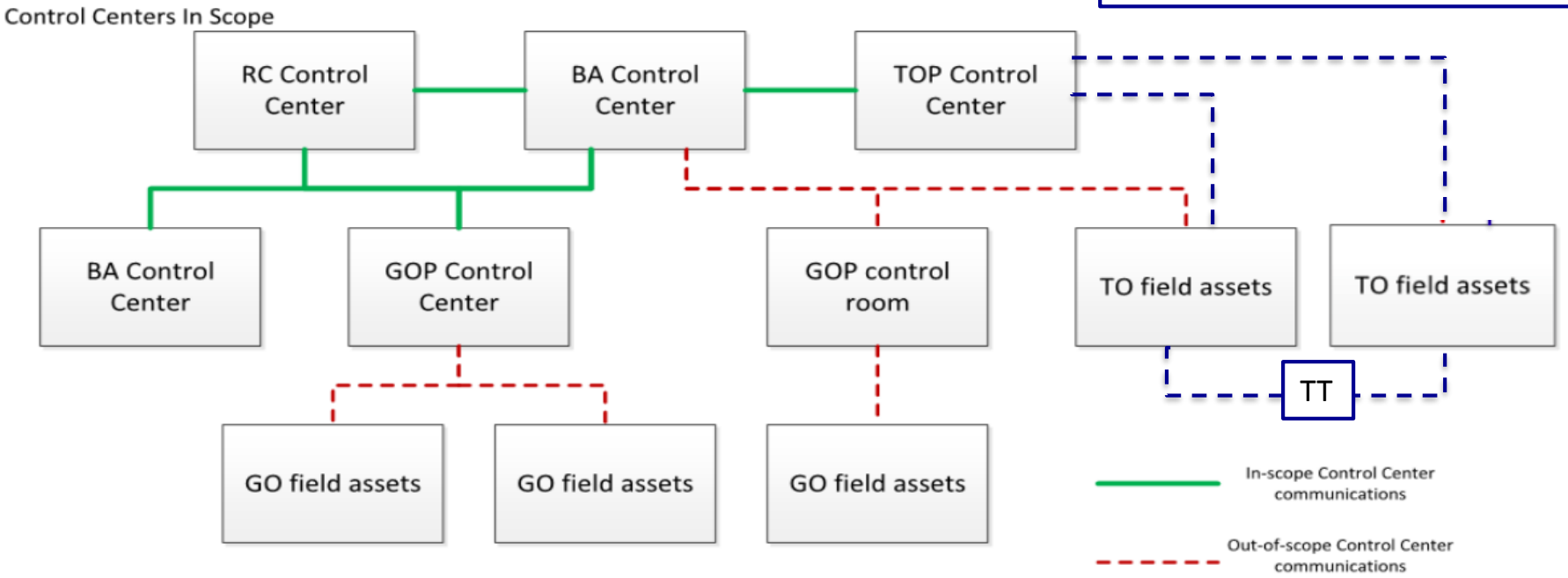
CIP-012-1 Draft 2

- CIP-012-1 Draft 1 was posted for comments and initial ballot through 9/11/2017
- CIP-012-1 Draft 2 is posted for comment through 12/11/2017
- CIP-012-1 Draft 2 will have an “additional ballot” window open from 12/1/2017 through 12/11/2017
- The draft RSAW for CIP-012-1 Draft 2 should be posted this week

Scope of CIP-012-1

- Due to the sensitivity of the data being communicated between Control Centers, as defined in the Glossary of Terms Used in NERC Reliability Standards, the standard applies to all impact levels (i.e., high, medium, or low impact).

Not addressed in CIP-012-1, but consider SCADA links to substations and TT links



(NERC, 2017 Aug 11, *Technical Rationale for CIP-012-1*, p. 5)

Applicability

- Own or operate a Control Center:
  - "One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in realtime to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations."
- There is no size limit to the Control Center
  - Any BES facility that meets the definition of Control Center will be in scope for this Requirement

Changes from Draft 1

- Title changed
  - *Communication Between Control Centers*
- Purpose statement modified and clarified
  - *To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring and control data transmitted between Control Centers.*
- Revised definition of “Control Center” dropped
- Applicability consolidated – all applicability criteria are now in the Applicability section
- Rationale section dropped
- R1 has more specifics regarding protections
- R2 is unchanged
- Implementation window increased from 12 months to 24 months after approval

It's All About The Data

- Mitigate the risk of loss of confidentiality or integrity of data transmitted between Control Centers
  - Real-time Assessment data
    - "An evaluation of system conditions using Real-time data to assess existing (pre-Contingency) and potential (post-Contingency) operating conditions. The assessment shall reflect applicable inputs including, but not limited to: load, generation output levels, known Protection System and Special Protection System status or degradation, Transmission outages, generator outages, Interchange, Facility Ratings, and identified phase angle and equipment limitations. (Real-time Assessment may be provided through internal systems or through third-party services.)"
  - Real-time monitoring and control data
  - Excludes verbal communications

Compliance Guidance Policy

Compliance Guidance Policy

November 5, 2015

Technical Rationale

- Explains the Standard Drafting Team intent
- This document does not standalone
- All depends upon the facts and circumstances

Implementation Guidance

- Implementation Guidance does not prescribe the only approach, but is intended to highlight one or more approaches that would be effective ways to be compliant with the standard. As Implementation Guidance is only meant to provide examples, entities may choose alternative approaches that better fit their situation.

Develop a Plan

- Identify data communications paths to be protected (implied requirement)
  - Real-time Assessment data
  - Real-time monitoring and control data
- Identify security protection for each path
- Identify demarcation (demarc) point for each path
- If path is to another entity, identify roles and responsibilities for each path

R1 Considerations (The Plan)

- Identification of security protection
  - Security protection could consist of logical protections, physical protections, or some combination of both
- Identification of demarcation point(s)
  - Identify clear demarcation of where the protection is applied to the in-scope data
- Identification of roles and responsibilities when the Control Centers are owned or operated by different Responsible Entities
  - Configuration of security protocols
  - Responding to communication failures
  - Responding to Cyber Security Incidents

Possible Compliance Evidence

R1 - One or more documented plans

- If more than one plan, make sure there are no gaps between the plans
- Ensure all the Parts of R1 are covered:
  - How to identify data paths to be protected
  - For each identified path, how it will be protected
  - For each identified path, where the protections will be applied
  - For each identified path, define the roles of responsibility
    - » Implementation
    - » Monitoring
    - » Maintenance
    - » Key management
    - » Etc.
  - For each identified path, define who is responsible for each role

R2 Considerations (Implementation of Plan)

- Identification of security protection
  - Physical: physical security measures in place protecting the communication link
    - CIP-006-6 R1.10 does not apply
  - Logical: device configuration which applies the security protection
  - Logical: monitoring the encryption service used to protect a communications link
- Identification of demarcation point(s)
  - Physical or logical diagram
- Identification of roles and responsibilities when the Control Centers are owned or operated by different Responsible Entities
  - Joint procedure, a memorandum of understanding or meeting minutes between the two parties where roles and responsibilities are discussed

Reference Models

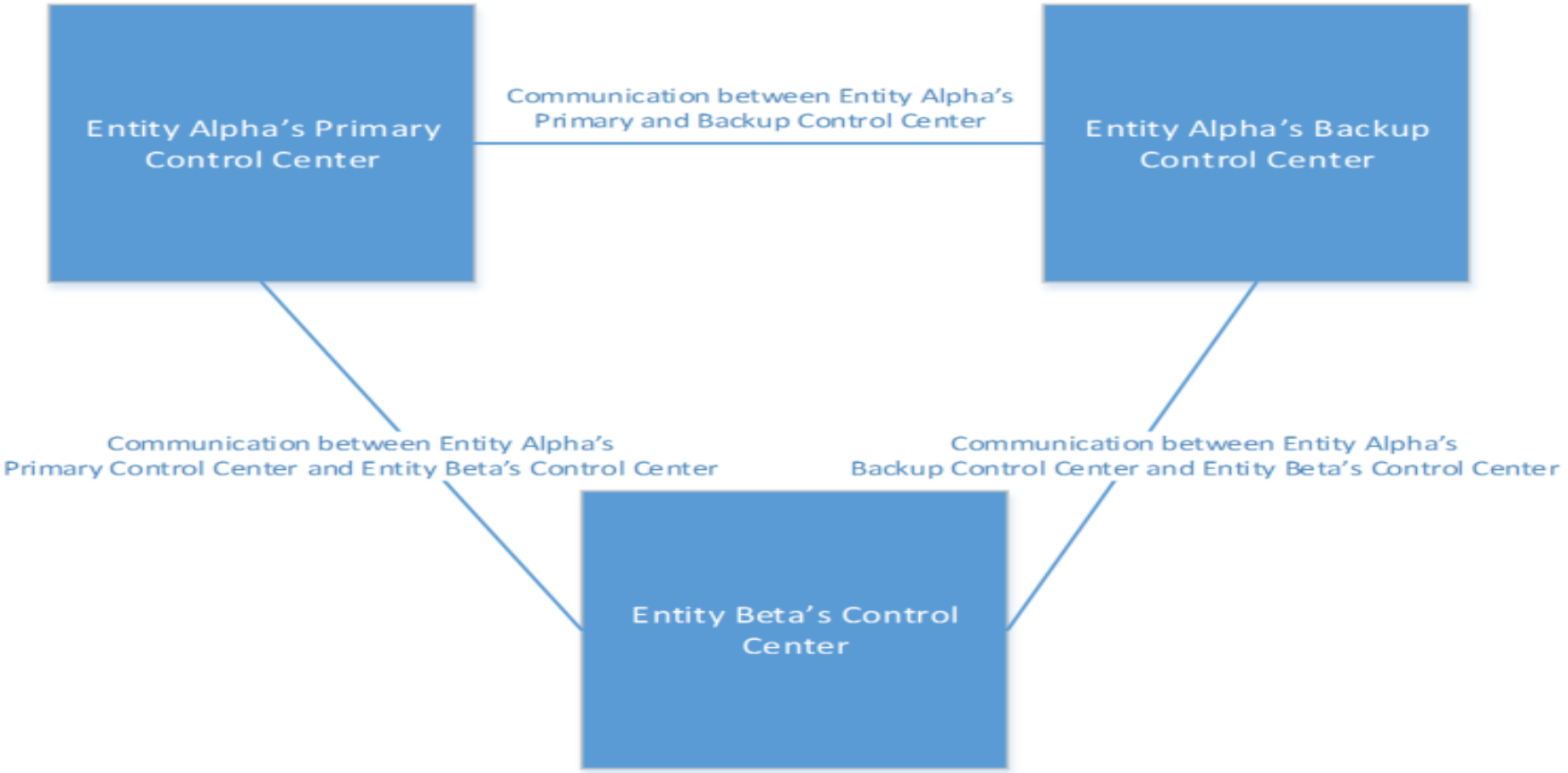


Figure 1: High Level Block Diagram of Reference Model Control Centers

Reference Models

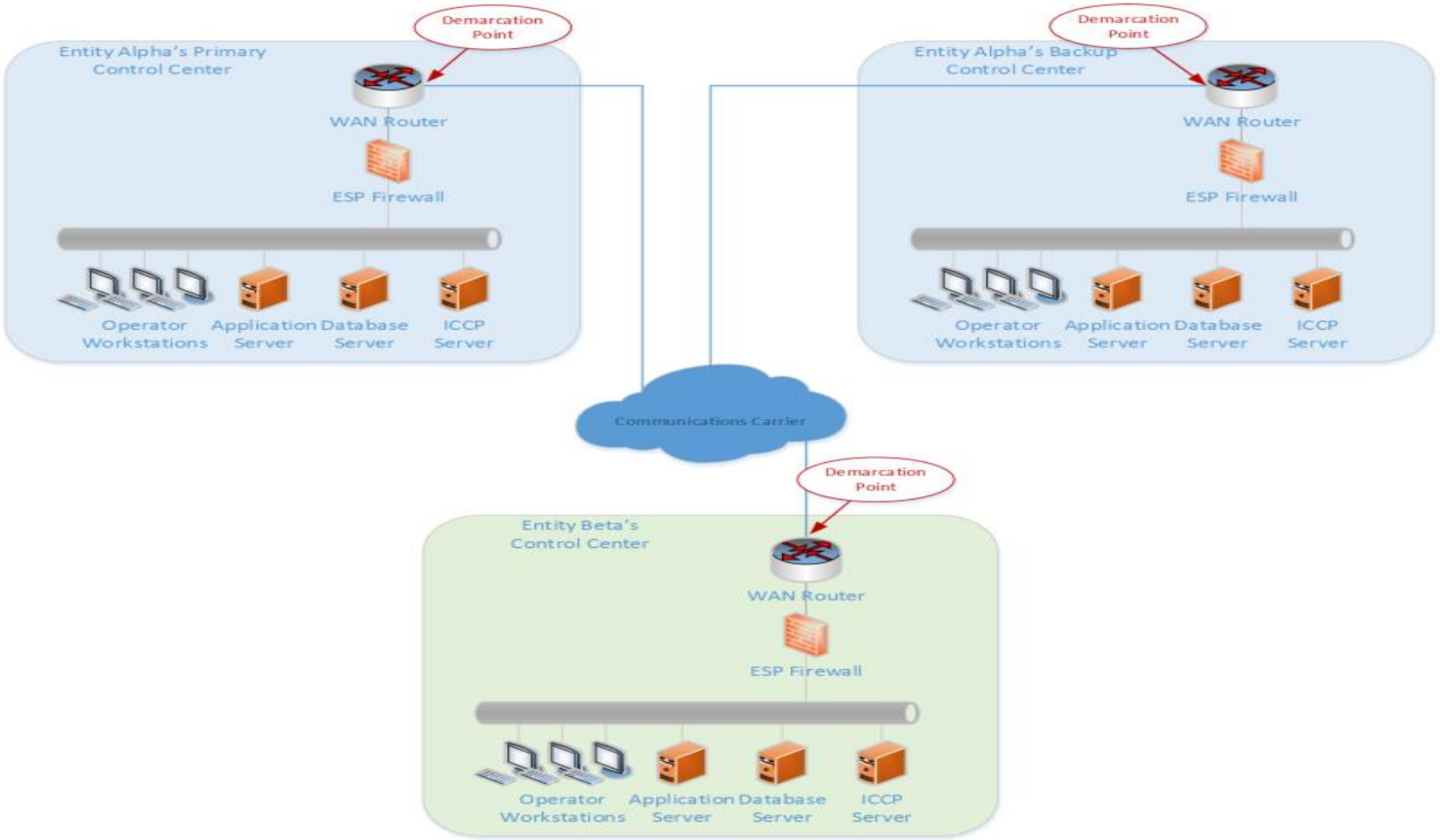


Figure 2: Network diagram and identification of demarcation points

Reference Models

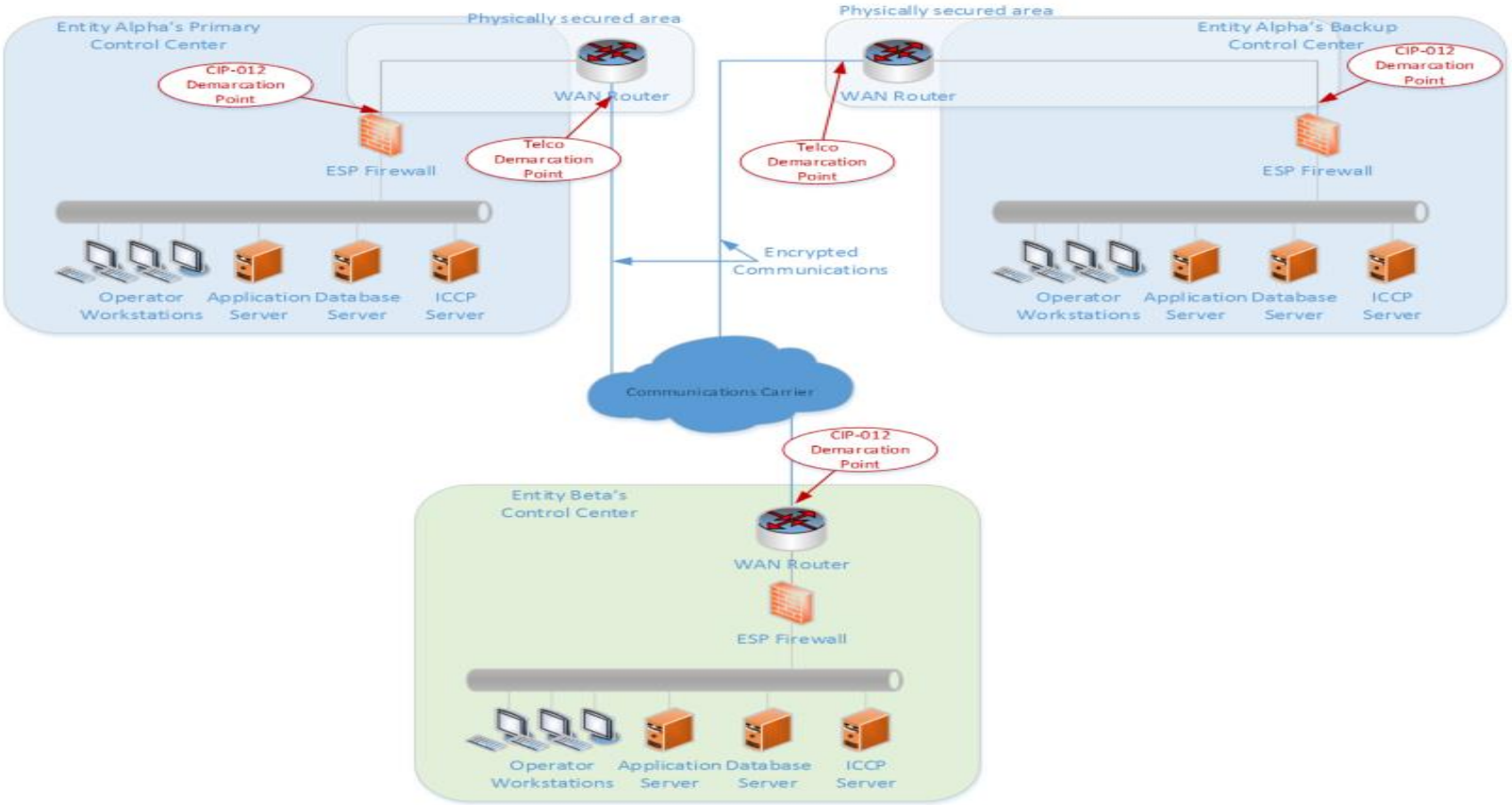


Figure 3: Network diagram using a combination of controls for CIP-012-1

3rd Party

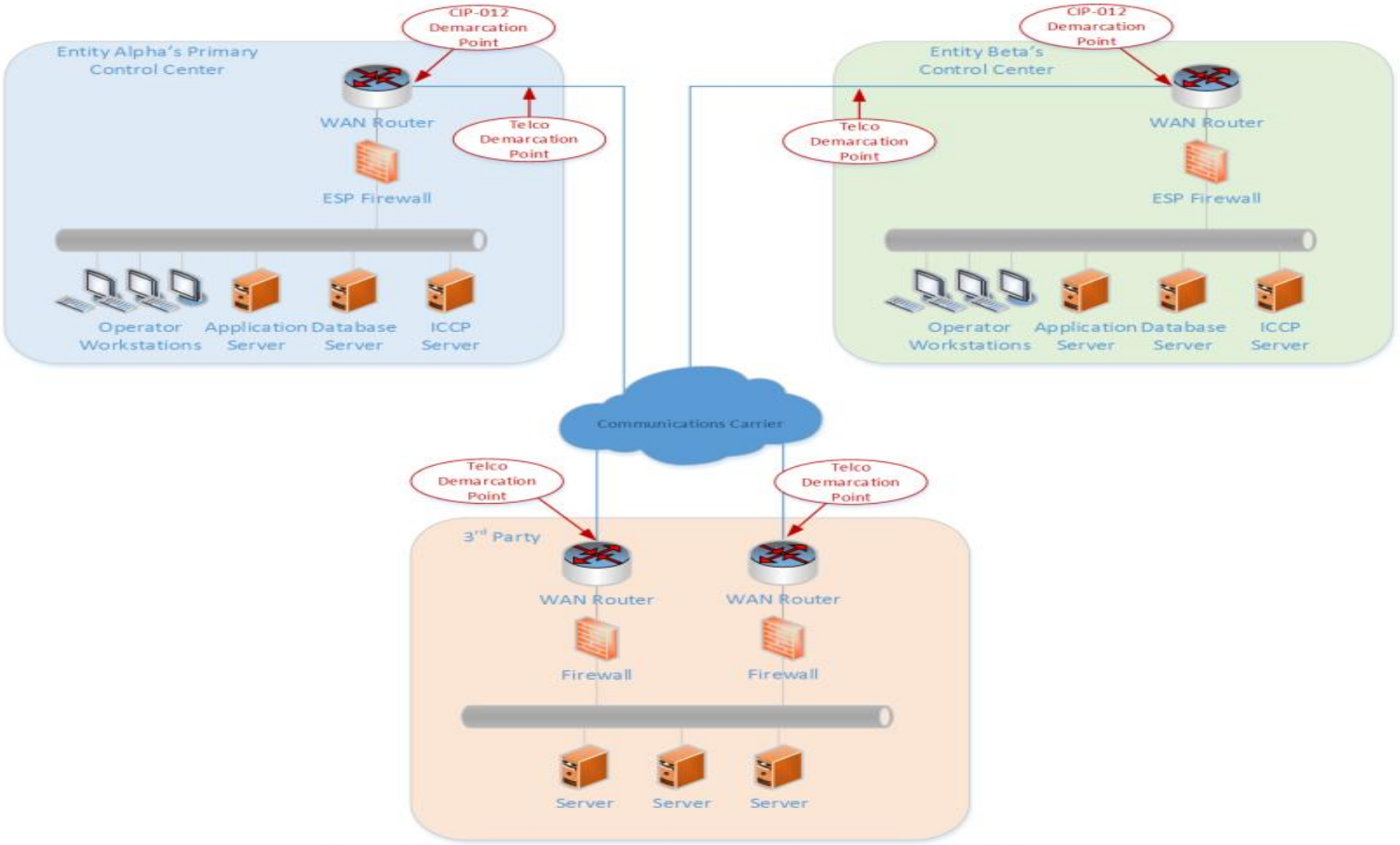


Figure 4: Network Diagram depicting communications through a 3rd party

Questions

- Does CIP-012-1 differentiate between entities that own the communication links/gear from those that do not?

- Does CIP-012-1 indirectly prescribe a specific solution?
  - 'Unauthorized Discloser or Modification'
  - Encryption is not explicitly required, but there may not be many alternatives that will meet the requirements from a logical approach
  - There are no provisions for Technical Feasibility Exceptions
  - Encryption is not always easy
    - Plan and Test! Test! Test!

RSAW

Registered Entity Response (Required):

Question 1: Does the Registered Entity own or operate a Control Center? ☐ Yes ☐ No

If no:

1. Provide evidence in the space that the Registered Entity does not own or operate one or more Control Centers. This evidence may include, but is not limited to:
   - Evidence that the Registered Entity does not own or operate a Control Center; or
   - **Evidence or a reference to evidence from the Registered Entity's CIP-002 compliance program that demonstrates the entity does not own or operate a Control Center.**
2. The remainder of this RSAW may be left blank.

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Stay Engaged

- WECC encourages all Responsible Entities who own or operate an applicable Control Center to comment on the second draft.
- Although the final version of CIP-012-1 is yet to be approved by both the NERC Board of Trustees and FERC, entities may choose to begin preparations based on the Draft 2 Requirement R1.

References

- Slide 5: (NERC, 2017 Aug 11, *Technical Rationale for CIP-012-1*, p. 5)
- http://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx

Questions and Contact Information

Morgan King

(801)819-7675 – Office

(801)608-6652 – Cell

mking@wecc.biz