NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security – Communications Between Control Centers

Implementation Guidance for CIP-012-1

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Introduction

The Commission issued Order No. 822 on January 21, 2016. Order 822 approved seven CIP Reliability Standards and new or modified definitions, and directed modifications be made to the CIP Reliability Standards. Among other items, the Commission directed NERC to "develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, the standard applies to all impact levels (i.e., high, medium, or low impact).

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both, to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment. Requirement R1 requires Responsible Entities to document one or more plans that protect Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers. The plan(s) must address how the Responsible Entity will mitigate the risk of unauthorized disclosure or modification of the applicable data. Requirement R2 covers implementation of the plan developed according to Requirement R1.

The Project 2016-02 SDT also drafted this Implementation Guidance document to provide examples of approaches to comply with CIP-012-1. 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[1].

Responsible Entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT developed Technical Rationale and Justification for CIP-012-1 document.

[1] NERC's Compliance Guidance Policy

Requirements

R1. *The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between any Control Centers. This requirement excludes oral communications. The plan shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers;

1.2. Identification of demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers; and

1.3. Identification of roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.

R2. *The Responsible Entity shall implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.*

General Considerations

General Considerations for R1

As noted in the Technical Rationale and Justification for CIP-012-1, the focus of Requirement R1 is on developing a plan to protect information that is critical to the real-time operations of the Bulk Electric System while in transit between applicable Control Centers. The number of plan(s) and their content may depend on a Responsible Entity's management structure and operating conditions. The Responsible Entity may document as many plans as necessary to meet its needs. For instance, a Responsible Entity may choose to document one plan per Control Center or it may choose to document everything in a single plan. A Responsible Entity may choose to document one plan for communications between Control Centers it owns and a separate plan for communications between its Control Centers and the Control Centers of a neighboring Entity. The number and structure of the plans is at the discretion of the Responsible Entity as long as the plan(s) include the required elements described in parts 1.1, 1.2, and 1.3 of Requirement 1.

Identification of Security Protection

Entities have latitude to determine which security protections are used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers and should identify those protections accordingly.

This security protection could consist of logical protection, physical protection, or some combination of both. To determine security protection, the requirement specifies that it must mitigate the risk of unauthorized disclosure or modification of applicable data.

Identification of Demarcation Point(s)

A Responsible Entity should consider its environment to determine an effective solution when identifying the demarcation points where security protections are applied. One approach to identifying a demarcation point is to place the demarcation point within the Control Center so the confidentiality and integrity of the data is protected throughout the transmission. The Responsible Entity can choose either a physical or logical demarcation point. Demarcation points identified by the Responsible Entity do not add additional assets to the scope of the CIP Reliability Standards. The demarcation point identification ensures that each Responsible Entity identifies clear demarcation of where the protection is applied to the in-scope data. Demarcation points may vary based on many factors such as impact levels of the Control Center, different technologies, or infrastructures.

Identification of Roles and Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

The Technical Rationale and Justification for CIP-012-1 identifies key considerations in the Control Center Ownership section when communicating between Control Centers with different owners or operators. Most if not all of the many relationships between Responsible Entities are unique. Consequently, there is no single way to identify roles and responsibilities for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers. Responsible Entities may consider identifying the roles and responsibilities for the following situations: (1) configuration of security protocols, (2) responding to communication failures, and (3) responding to Cyber Security Incidents.

General Considerations for R2

Given the format of the requirements, the majority of the documentation is required under R1 while R2 requires the implementation of the plan developed for R1. Compliance with R2 is established by implementing the protection identified in a Responsible Entity’s R1 plan. The sections below outline examples of evidence that may be provided in order to demonstrate the implementation of Entity Alpha’s CIP-012-1 R1 plan.

Identification of Security Protection

Implementation of the security protection can be demonstrated in many ways. If physical protection is used, a Responsible Entity may demonstrate implementation through a floor plan which identifies the physical security measures in place protecting the communication link. If logical protection is used, a Responsible Entity may demonstrate implementation through an export of the device configuration which applies the security protection. Alternatively, a Responsible Entity may demonstrate implementation through monitoring of the security control such as a report generated from an automated tool that monitors the encryption service used to protect a communications link.

Identification of Demarcation Point(s)

Identification of demarcation point(s) could be demonstrated with a diagram (physical or logical) or a list. This diagram or list could be included within the plan developed for R1. A label could also be used to identify a device as a demarcation point.

Identification of Roles and Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

Implementation of roles and responsibilities could also be demonstrated in many ways. Some examples include a joint procedure, a memorandum of understanding or meeting minutes between the two parties where roles and responsibilities are discussed.

Reference Models

For this Implementation Guidance, the SDT considers a basic reference model of Primary and Backup Control Centers (Entity Alpha) to illustrate concepts necessary to demonstrate compliance. These Control Centers communicate to each other and to a neighboring entity's Control Center (Entity Beta) in configurations outlined by the diagrams in this section. The SDT recognizes that the reference models do not contain many of the complexities of a real Control Center. For this Implementation Guidance, the registration or functions performed in the reference model Control Center are also not considered. A high level block diagram of the basic reference model is shown below in Figure 1. This Implementation Guidance is developed from the perspective of Entity Alpha.

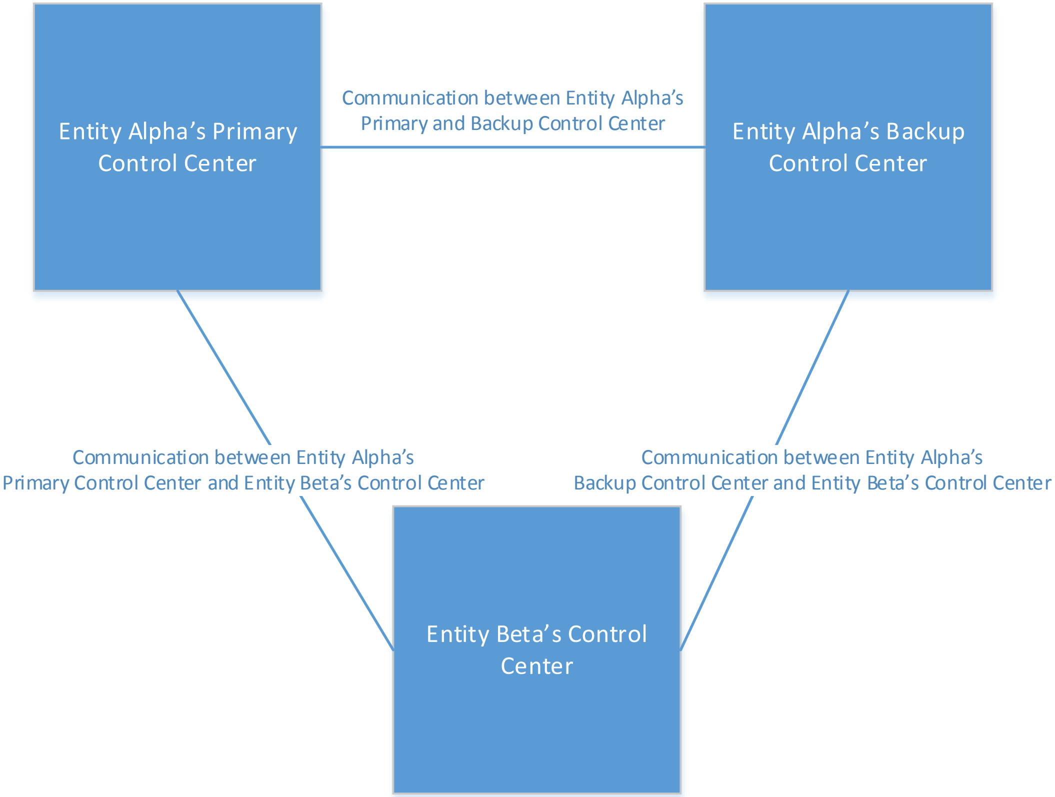
Entity Alpha's Primary Control Center
Communication between Entity Alpha's Primary and Backup Control Center
Entity Alpha's Backup Control Center
Communication between Entity Alpha's Primary Control Center and Entity Beta's Control Center
Communication between Entity Alpha's Backup Control Center and Entity Beta's Control Center
Entity Beta's Control Center

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

Reference Model Discussion for Requirement R1

Requirement R1 requires the development of a documented plan. To comply with requirement R1, one approach to a plan is to first determine which communications require protection pursuant to CIP-012-1. There are multiple ways to identify an entity's scope in R1. For example, Entity Alpha in the reference model may first identify the Control Centers with which it communicates. Entity Alpha would determine that there are three: Entity Alpha's Primary Control Center, Entity Alpha's Backup Control Center, and Entity Beta's Control Center. Entity Alpha does not need to consider whether Entity Beta further shares its data with another Entity. That is the responsibility of Entity Beta and is outside of Entity Alpha's purview. Additionally, Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1.

Now that Entity Alpha has identified the Control Centers with which it communicates, Entity Alpha identifies either: (1) the Real-time Assessment and Real-time monitoring and control data; or (2) communication links which are used to transmit Real-time Assessment and Real-time monitoring and control data between Control Centers. In either case, Entity Alpha may find it useful to refer to the data specification for Real-time

Assessment and Real-time monitoring data identified in TOP-003-3 and IRO-010-2. For this reference model scenario, identifying the communication links used to transmit Real-time Assessment and Real-time monitoring and control data may be the most straightforward approach. Through an evaluation of communication links between Control Centers and an evaluation of how it transmits and receives Real-time Assessment and Real-time monitoring and control data, Entity Alpha determined that it communicates applicable data between its primary and backup Control Centers across a single communication link. Entity Alpha also determined that it communicates applicable data to and from Entity Beta's Control Center across one of two links that originate from either Entity Alpha's primary or backup Control Center using the Inter-Control Center Communications Protocol (ICCP).

With an identified scope of communications links, Entity Alpha now considers the three required elements of its required communications between Control Centers for its plan.

Identification of Security Protection

- Entity Alpha must ensure that protection is applied at the CIP-012-1 demarcation point. The protection must also meet the security objective of mitigating the risk of unauthorized disclosure or modification of applicable data while in transit between Control Centers for the entire distance between CIP-012-1 demarcation points. In a simple case where the demarcation point is sufficiently close to the Control Center, such as within the Physical Security Perimeter of the Control Center, Entity Alpha may use a single security protection method to meet the security objective. For this case, shown in Figure 2, Entity Alpha documents in its plan that it uses a Virtual Private Network (VPN) connection across a private leased communication circuit for each of its three in-scope communication links. To meet the security objective, Entity Alpha further states that its VPN uses Internet Protocol security (IPsec) with AES-128 encryption.
- For more complex scenarios, Entity Alpha may need to use a combination of security controls. For instance, in Figure 3, Entity Alpha uses a combination of physical security controls (physical access control) and logical security controls (encrypted communications consistent with the first scenario above) to meet the security objective.
- The complexity increases when Entity Alpha and Entity Beta exchange data through a 3rd party, such as in Figure 4. In this scenario, Entity Alpha again uses a combination of logical controls. First, encrypted communications are used between the CIP-012-1 demarcation point at Entity Alpha and extended to the 3rd party WAN router. Then, a number of security controls may be leveraged such as network segmentation and system access control to protect the data as it transits the 3rd party network. Finally, encrypted communications is used again to protect the data as it transits between the 3rd party network and the CIP-012-1 demarcation point at Entity Beta.
- While these scenarios are all specific to communication links, it is possible that Entity Alpha and Entity Beta achieve the security objective by applying protection to the data rather than the communication links. In this scenario, the application enabling the data exchange between Control Centers may be capable of applying security controls directly to the data. These security controls mitigate the risk of unauthorized disclosure or modification of applicable data rather than relying on lower level network services to provide this security. For instance, Entity Alpha and Entity Beta may apply security protection at the application layer by using Secure ICCP to exchange applicable data. According to a report released by Sandia National Labs[2], Secure ICCP provides "data integrity indirectly by providing a cryptographic checksum…Secure ICCP provides data confidentiality by encrypting ICCP data exchanges." Methods other than Secure ICCP could also be used to apply security protection to the data at the application layer.
- It is theoretically possible that Entity Alpha and Entity Beta could exchange Real-time Assessment data between Control Centers by email. In that scenario, one approach may be for Entity Alpha to email the

[2] https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/19-Secure_ICCP_Integration.pdf

applicable data to Entity Beta's Control Center in a protected container such as an encrypted zip file. Entity Alpha and Entity Beta can then exchange the password to that encrypted container through another method, such as by phone. While the notional example of protecting data exchanged by email is a useful illustration of how to achieve the security objective of CIP-012-1, it is extremely unlikely to be used in practice. The characteristics of email communication are inconsistent with the requirements of Real-time data exchange.

Identification of Demarcation Point(s)

- Figure 2 shows the identification of CIP-012-1 demarcation points for the Entity Alpha reference model. Entity Alpha has identified its demarcation point at each of its Control Centers to be the external Ethernet interface on the WAN router where the security protection is applied. It has also coordinated with Entity Beta to identify a similar demarcation point at Entity Beta's Control Center.
- In some cases, it may be helpful to identify both the CIP-012-1 demarcation points and the telecommunications carrier (telco) demarcation point. Figure 3 provides such an example where the telco demarcation point may not be within the Control Center. In this scenario, Entity Alpha identifies the CIP-012-1 demarcation point to be a point on the communications path adjacent to the outside interface on the ESP firewall. Entity Alpha has also identified the telco demarcation point at a point in the telecommunications cabling connecting to Entity Alpha's WAN router, perhaps at a punch down block for example. In Figure 3, the telco demarcation point is inside the same room as the WAN router. The telco demarcation points are referenced in the drawing for clarity, but are not part of the plan.
- Figure 4 shows the identification of possible CIP-012-1 demarcation points and telco demarcation points when Entity Alpha and Entity Beta transmit the applicable data through a third party.
- The data-centric scenario described above is less intuitive for identifying demarcation points. If security protection is applied at the application layer (such as Secure ICCP), Entity Alpha could reasonably identify the application or service applying the security (such as the Secure ICCP service) as the demarcation point.

Identification of Roles and Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

Entity Alpha and Entity Beta may determine they each are responsible for one end of the VPN configuration on their respective WAN routers. Entity Alpha and Entity Beta have agreed to a 30 character pre-shared key for IPSec authentication and have exchanged contact information for their Network Operations Centers to enable a coordinated response to any communication failures. They have also exchanged contact information for their Security Operations Centers to enable a coordinated response to any suspected Cyber Security Incidents.

Rather than use a pre-shared key, Entity Alpha and Entity Beta may decide to use digital certificates for the IPSec authentication using a trusted certificate authority. In that scenario, Entity Alpha and Entity Beta would agree on who is the party responsible for managing the certificate authority.

When using a third party as shown in Figure 4, Entity Alpha and Entity Beta will need to define who is responsible for each part of the connection between them. Each entity may determine they are responsible for only the connection from their CIP-012-1 demarcation point to the telco demarcation point at the 3rd party. The 3rd party may take responsibility for protecting the data transiting its network.

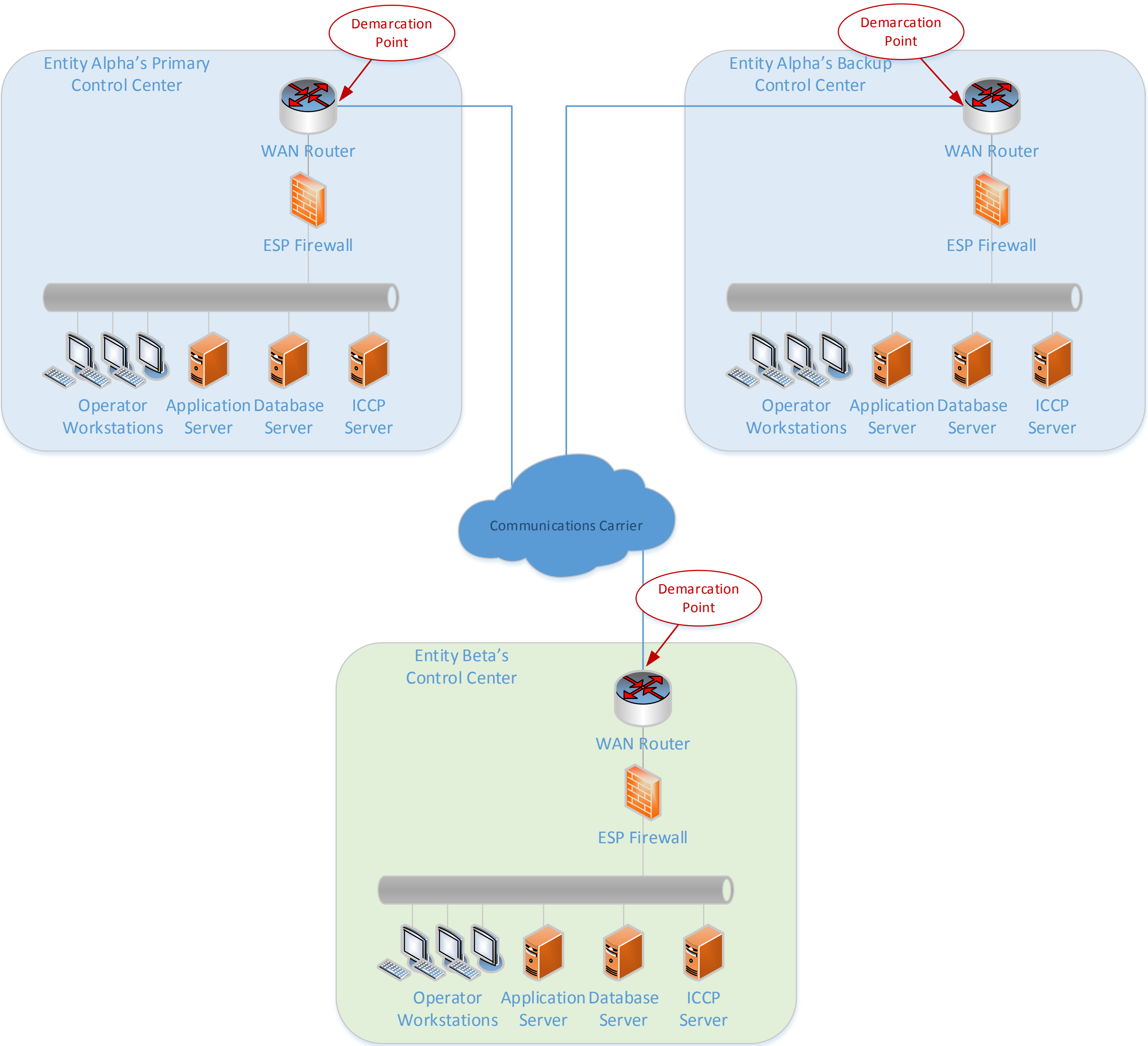

Figure 2: Network diagram and identification of demarcation points

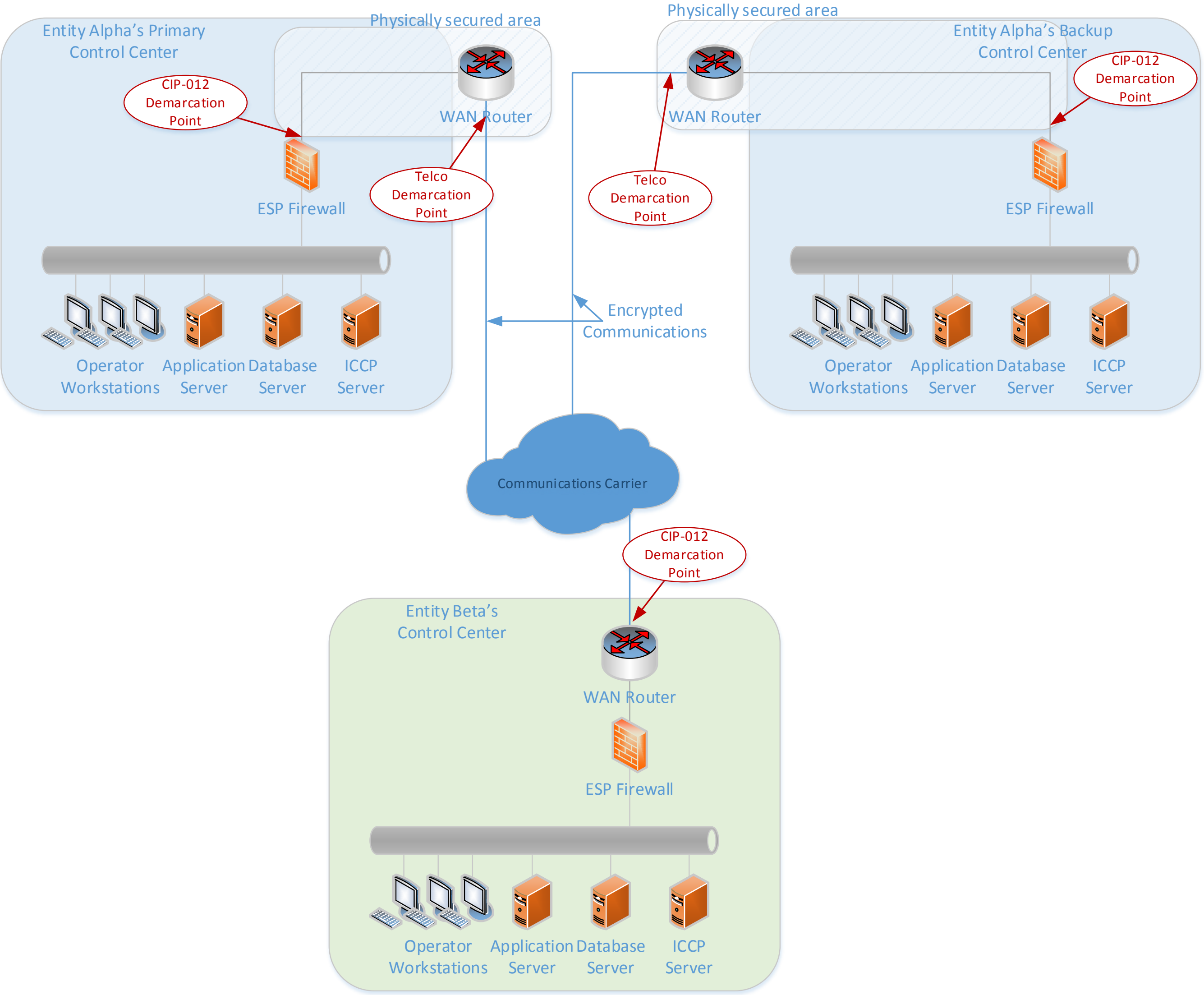

Figure 3: Network diagram using a combination of controls for CIP-012-1

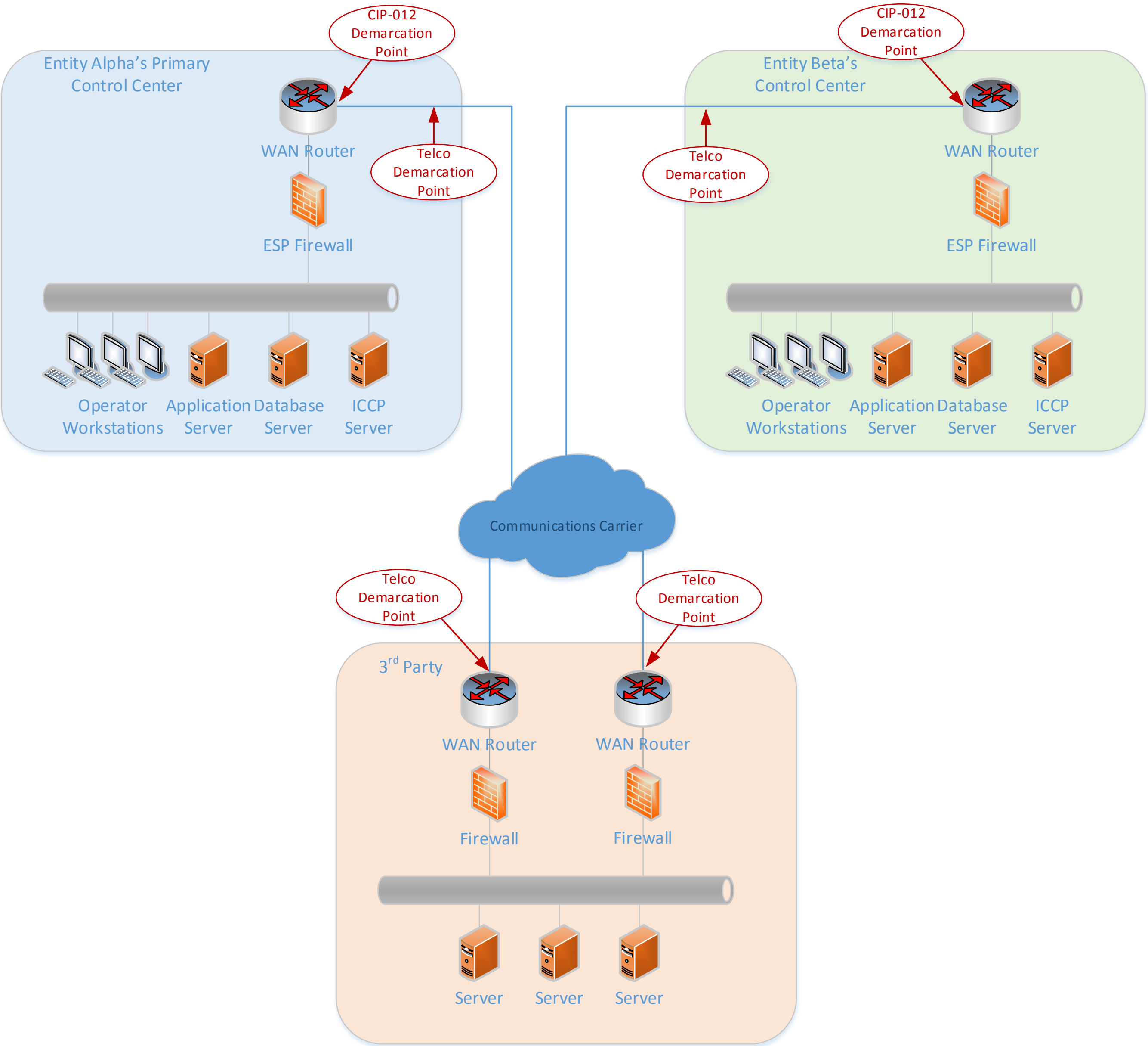

Figure 4: Network Diagram depicting communications through a 3rd party

Reference Model Discussion for Requirement R2

Entities must demonstrate implementation of their R1 plan. The sections below outline examples of evidence that may be provided to demonstrate the implementation of Entity Alpha's CIP-012-1 R1 plan.

Identification of Security Protection

Entity Alpha may demonstrate security protection implementation through the WAN router configuration which shows that a site-to-site IPSec VPN with AES-128 encryption is in place.

When physical security controls are used, Entity Alpha may demonstrate the implementation of physical protection using a floorplan diagram showing the physical access controls in place.

Identification of Demarcation Point(s)

Entity Alpha may demonstrate the identification of demarcation points through a network diagram very similar to that shown in Figure 2.

Identification of Roles and Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

Entity Alpha may demonstrate the implementation of roles and responsibilities with Entity Beta through a memorandum of understanding (MOU) signed by both parties.

References

Mitre Common Weakness Enumeration (CWE™) list of software weakness types
https://cwe.mitre.org/data/definitions/327.html

Cryptographic Standards and Guidelines
https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines

NIST Special Publication 800-175B
Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf

Guide to Cryptography
https://www.owasp.org/index.php/Guide_to_Cryptography#Symmetric_Cryptography